Security Basics

Sponsored by: CDNetworks

Start Time	Title	Presenter
8:30 AM	Introduction	Hugh Thompson
8:45 AM	Security Industry and Trends	Hugh Thompson
9:30 AM	Authentication Technologies	Michael Poitner
10:15 AM	Break	
10:30 AM	Governance, Risk and Compliance	Dennis Moreau
11:15 AM	Application Security	Jason Brvenik
12:00 PM	Lunch	
1:15 PM	Crypto 101/Encryption Basics, SSL & Certificates	Benjamin Jun
2:00 PM	Firewalls and Perimeter Protection	Dana Wolf
2:45 PM	Break	
3:00 PM	Viruses, Malware and Threats	Tas Giakouminakis
3:45 PM	Mobile and Network Security	Mike Janke

RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Introduction and A Look at Security Trends

SESSION ID: SEM-MO1

Hugh Thompson, Ph.D.

Program Committee Chairman, RSA Conference

Agenda

Intro to Information Security

Economics of Information Security

Security Trends

The Shifting IT Environment

(…or why security has become so important)

Shift: Compliance and Consequences

- The business has to adhere to regulations, guidelines, standards,…
  - SAS 112 and SOX (U.S.) – upped the ante on financial audits (and supporting IT systems)
  - PCI DSS – requirements on companies that process payment cards
  - HIPAA, GLBA, BASEL II, …, many more
- Audits are changing the economics of risk and create an "impending event"

Hackers *may* attack you but auditors *will* show up

- Disclosure laws mean that the consequences of failure have increased
  - Waves of disclosure legislation

Shift: Technology

- System communication is fundamentally changing – many transaction occur over the web
- Network defenses are covering a shrinking portion of the attack surface
- Cloud is changing our notion of a perimeter
- Worker mobility is redefining the IT landscape
- Shadow IT is becoming enterprise IT
- The security model has changed from good people vs. bad people to enabling partial trust
  - There are more “levels” of access: Extranets, partner access, customer access, identity management, …

Shift: Attackers

- Cyber criminals are becoming organized and profit-driven
  - An entire underground economy exists to support cybercrime
- Attackers are shifting their methods to exploit both technical and human weaknesses
- Attackers after much more than traditional monetizable data (PII, etc.)
  - Hacktivism
  - State-sponsored attacks
  - IP attacks/breaches

Shift: Customer expectations

- Customers, especially businesses, are using security as a discriminator
- In many ways security has become a non-negotiable expectation of businesses
- Banks, photocopiers, pens, etc. are being sold based on security…
- Security being woven into service level agreements (SLAs)

Big Questions

- How do you communicate the value of security to the enterprise (and management)?
- How do you measure security?
- How do you rank risks?
- How do you reconcile security and compliance?
- How can you be proactive and not reactive?
- What changes are likely in privacy laws, data sovereignty, trust?
- What about big issues in the news like APT's, hacktivism, leaks, DDoS attacks, …? How should/can we adapt what we do based on them?

The Economics of Security

Hackernomics (*noun*)

A social science concerned chiefly with description and analysis of attacker motivations, economics, and business risk. Characterized by

5 fundamental immutable laws and 4 corollaries

Law 1

Most attackers aren't evil or insane; they just want something

Corollary 1.a.:
We don't have the budget to protect against evil people but we *can* protect against people that will look for weaker targets

Law 2

Security isn't about security. It's about mitigating risk at some cost.

Corollary 2.a.:
In the absence of metrics, we tend to over focus on risks that are either familiar or recent.

Law 3

Most costly breaches come from simple failures, not from attacker ingenuity

Corollary 3.a.:
Bad guys can, however, be VERY creative if properly incentivized.

The CAPTCHA Dilemma

Completely

Automated

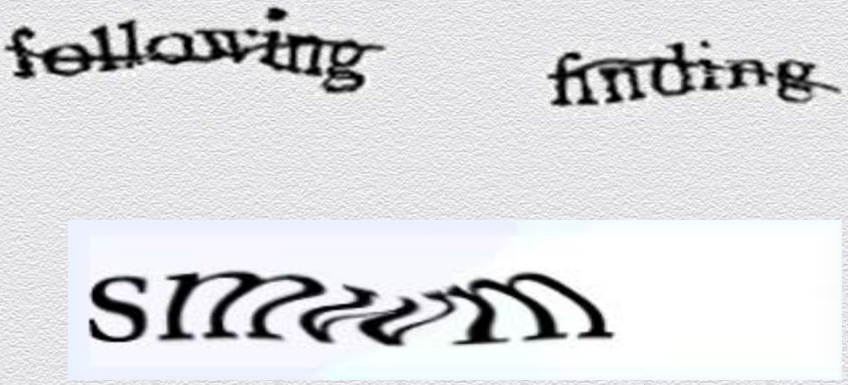
Public

Turing test to tell

Computers and

Humans

Apart



Law 4

In the absence of security education or experience, people (employees, users, customers, …) naturally make poor security decisions with technology

Corollary 4.a.:

Systems needs to be **easy to use securely and difficult to use insecurely**

Law 5

Attackers usually don’t get in by cracking some impenetrable security control, they look for weak points like trusting employees

A Visual Journey of Security Trends

2008


Management
Identity
New
Web
Enterprise
Standards
Attacks
Services
Data
Authentication
Protection
Using
Digital
Threat
Access
Electronic
World
Challenges
Strategies
Information
Software
Control
Implementing
Case
Technology
Practices
Application
Federated
Compliance
SOA
Approach
Network
Vulnerabilities
Risk
Internet
Bank
Policy
Infrastructure
Key
Government
Deployment
Online
Consumer
Analysis
Environment
Based
Contracts
Mobile
Law
Privacy
Generation
Time
Breaking
Intelligent
Defense
Development
Cyber
Solving
Integration
Experience
Lessons
Architecture
Biometrics
Signatures
Best
Business
Assessment
Solutions
Techniques
Initiatives
Real
Systems
Industry
Engines
Money
Panel
Global
Study
Trust
Debate

2009


Risk
Application
Threat
Compliance
Network
Management
Web
Identity
Data
Virtualization
Business
Access
Information
Enterprise
Protection
Cloud
Services
Approach
Standards
PCI
Software
Encryption
Development
Implementing
Vulnerability
Testing
Attacks
Practices
Malware
Mobile
Analysis
World
Using
Future
Cyber
New
Control
Challenges
Lessons
Key
Based
Case
Policy
Privacy
Learned
Building
Systems
Endpoint
Authentication
Solutions
Strategy
Trust
Infrastructure
Social
Effective
User
Prevention
Time
Program
Changing
Integrating

2010


Management
Identity
Enterprise
Authentication
Business
Protecting
Virtualization
Cloud
Information
Access
Approach
Solutions
Network
Data
New
based
Users
Threats
Control
Architecture
Strategies
Risk
Enabling
systems
Certificate
Measurement
Compliance
SaaS
Using
Building
Implementation
Encryption
Awareness
Lifecycle
Mobility
analysis
Federated
Trust
PKI
VoIP
Model
Key
Applications
Policy
Privacy
Success
Learned
Service
Vulnerability
Computing
Outsourcing
Know
Environments
Cyber
Malware
time
Lessons
World
Practical
digital
Introduction
Metrics
Complexity
Web
smart
Devices
Research
Analyzing
Challenges
Design
fraud
Banks
End
Self
Converged
Internet
Cases
High
Leaks
Integrated
Education
Making
Roles
Silos
Methods
Transforming
Assessment
Today
Programs
provider
Center
Operations
Cards
True
Consumer
Biometrics
Reputation
Internal
Signing
Deploying
Technology
Steps
Behavioral
stacks
Year

2011


Management
Cloud
Risk
Data
Cyber
Identity
Network
Threat
Enterprise
Practices
Application
Information
Attacks
New
Compliance
Mobile
Virtual
Web
Building
Malware
Using
Protecting
Strategy
Encryption
Business
Authentication
Infrastructure
Vulnerability
Software
Privacy
Trusted
Development
Devices
World
Challenges
Social
Lessons
Control
Best
Program
Service
Based
Environment
Approach
Solutions
Intelligence
Advanced
PCI
Public
Access
Computing
Architecture
Key
Analysis
Making
Lifecycle
Case
Integrated
Real
Effective
Critical
Continuous
Awareness
Assurance
Value
Open
Time
Study
Future
Government
Internet
Metrics
Insider
Prevention
Process
Leveraging
Generation
Framework
Fighting
Understanding
Changing
Monitoring
Technology
Global
Private
Success
Implementing
User
Policy
Research
Forensics
Wireless
Source
Certification
Assessment
Banking
Program
Operational
Legal
Don
Digital
War
Federal
Testing
Audit
Impact
Training
Systems
State
Meeting
Defense
Media
Applying
Industry
Learned
Center
Requirements
Deployment
Sharing
Internal
Problem
Tokenization
Automating
Hacking
Privilege
Enabling
Resilient
Healthcare
Fraud
App
High
Innovation
Collaboration
Cybercrime
Tips

2012


Mobile
Threat
Management
Cloud
Data
Application
Cyber
Risk
Attacks
Enterprise
Compliance
Software
Virtualization
Network
Information
New
Using
Building
Protecting
Strategy
World
Malware
Web
Control
Identity
Trust
Business
Device
Challenge
Breach
Design
Authentication
Development
Insider
Users
Social
Access
Services
Making
Apps
Forensics
Integrating
Internet
Standards
Operational
Convergence
Infrastructure
Time
State
Smart
Practices
Testing
Best
Defense
Intelligence
Encryption
Vulnerabilities
Advanced
Exploiting
Privacy
Lessons
Technology
Government
Approach
Policy
Response
APT
Hacking
Computing
Defending
Cybersecurity
Digital
Engineering
Future
Real
Changed
Online
Learned
Know
Tokenization
Solutions
Cards
Assurance
Firewalls
Live
Problem
Evolution
Persistent
Banking
Public
Effective
Organization
Legal
Work
Case
Analysis
Certification
Hackers
Program
Getting
Systems
Help
Key
PCI
Detection
Awareness

2013


Cloud
Management
Mobile
Data
Threats
Network
Attacks
Risk
Cyber
Information
Enterprise
Malware
Application
Protection
BYOD
Big
New
Identity
Business
Privacy
Control
Building
Approach
Devices
Vulnerability
Intelligence
Defense
Using
Social
Trust
Encryption
Advanced
Compliance
Virtual
Software
Breach
Hacking
Key
Real
Fraud
Program
Service
Detection
Future
Web
Learned
Lessons
Development
Authentication
World
Practices
Testing
Solutions
Analysis
Challenges
Critical
Infrastructure
Improving
Legal
Apps
Insider
Code
Strategy
Automated
Response
Policy
Public
Best
Case
Analytics
Sharing
Mitigating
Model
Know
Effective
Standards
Framework
Defending
Awareness
Incident
Environments
Internet
Government
Prevention
Systems
Metrics
Access
Based
Password
Global
Chain
Assessment
Cybersecurity
Technology
Study
Work
Private
Operations
Compromise
Monitoring
Making
Evolution
Getting
DDoS
Forensics
State
Time
PCI
APT
CISO
Users
Exploit
Industry
Smart
Professionals
Hackers
Integrated
Implementing
Computing
Perspective
Success
Emerging
Trends
Infosec
Understanding
Cost
Platform
Visibility
Game
Communication
Behavioral
Think
Android
Layered
Matters
Vendor
Media
Reports
Battle
Live
need
Bring
Year
Product
Preparing
Identity
Techniques
Federated
OAuth
Authorization
Physical
Firewall
Online
Auditing
Crime
Deployment
Architecture
Good
Center
Don
Party
SIEM
Providers
Really
Tools
Come
Dead
Open
Drive
War
Point
Law
Fail
Customer
Breaking
Win
Generation
Panel
Fighting
People
Problem
Reality
Issues
Applying
Requirements
Story
Secret
Measuring
vs
Step
Certificate
Want
National
Microsoft
Black
Source
Way
Supply
Continuous
Corporate
Banking
Persistent
Digital
Things
Evolving
Self
Today
Look
Implications
Engineering
Static
Industry
Stop
Insecurity
Windows
Warfare
Enabled
Long
Content

2014


technology
development
world
program
industry
implementation
management
share
threats
approach
based
cloud
new
data
users
tools
ways
malware
detection
help
prevent
intelligence
infrastructure
defense
advanced
systems
control
address
real
practices
need
government
work
software
organizations
risk
business
process
breach
critical
strategy
cyber
attacks
privacy
solutions
mobile
information
access
best
techniques
issues
create
environment
years
case
challenges
authentication
traditional
successful
different
change
policy
model
time
social
experts
future
trust
cybersecurity
research
analysis
protect
response
applications
enterprise
network
methods
vulnerabilities
services
operations
devices
including
identity
effective
requirements

Enjoy the rest of the conference!!

Security Basics

Sponsored by: CDNetworks

Start Time	Title	Presenter
8:30 AM	Introduction	Hugh Thompson
8:45 AM	Security Industry and Trends	Hugh Thompson
9:30 AM	Authentication Technologies	Michael Poitner
10:15 AM	Break	
10:30 AM	Governance, Risk and Compliance	Dennis Moreau
11:15 AM	Application Security	Jason Brvenik
12:00 PM	Lunch	
1:15 PM	Crypto 101/Encryption Basics, SSL & Certificates	Benjamin Jun
2:00 PM	Firewalls and Perimeter Protection	Dana Wolf
2:45 PM	Break	
3:00 PM	Viruses, Malware and Threats	Tas Giakouminakis
3:45 PM	Mobile and Network Security	Mike Janke

RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Authentication – Current state and future

SESSION ID: SEM-M01

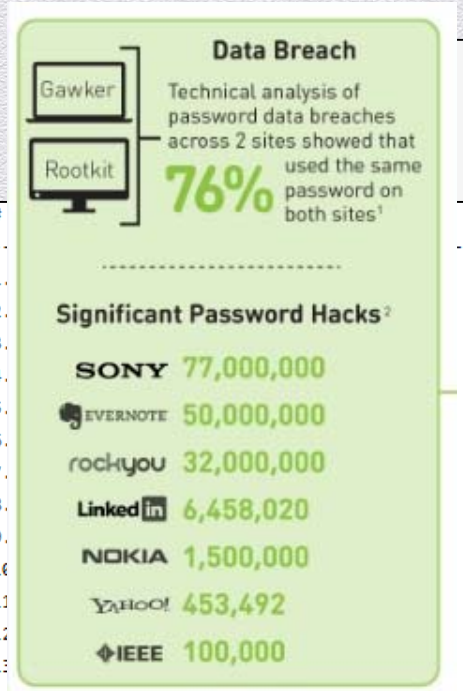
Michael Poitner

Global Segment Marketing Director
NXP Semiconductors

Table of Contents

- Introduction to Authentication
- Beloved passwords
- Overview Authentication Methods
- User vs. Device Authentication
- FIDO Alliance
- Overview NXP Semiconductors

Passwords are obsolete



#		Plaintext
1.		123456
2.		123456789
3.		password
4.		adobe123
5.		12345678
6.		qwerty
7.		1234567
8.		111111
9.		photoshop
10		123123
11		1234567890
12		000000
13		abc123
14		1234
15.	56744 5wEAInH22i4=	adobe1

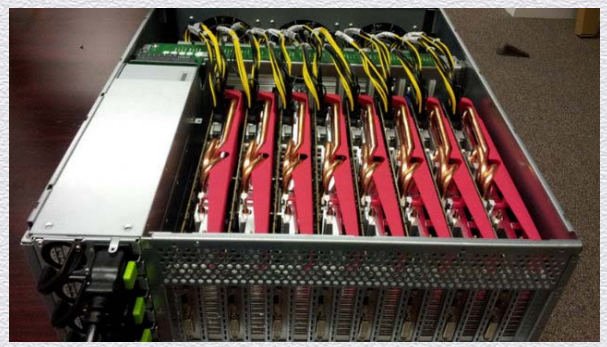
Too many t

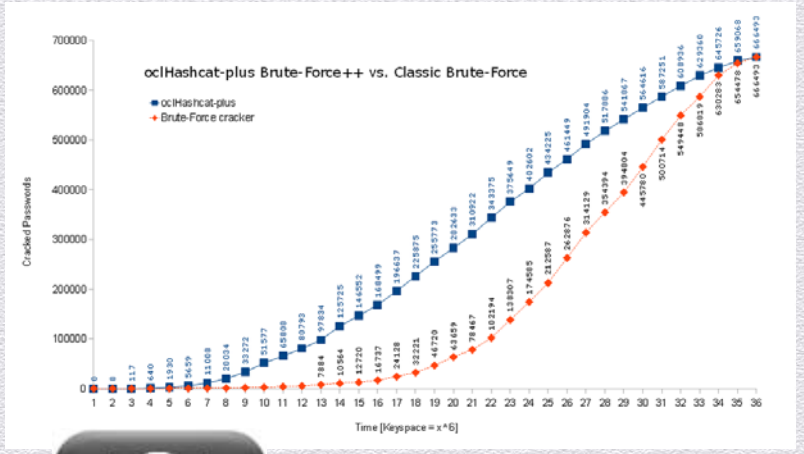
For 20 Years the Nuclear Launch Code at US Minuteman Silos Was 00000000

PHISHED KEYLOGGED

BruteForce++ is getting scary

- 8 digits (NTLM) takes now 5.5h (348B NTLM hashes per second)
- 14 digits (LM) takes 6min
- Dictionaries (110M+ entries)
- L1nk3d1n or xxxxxxx12 does not cut it anymore
- Rain bow tables, Amazon EC2
- John the ripper and Hashcat (GPU)
- Server side (Hash, salt, bcrypt, HSM)





Other ways to authenticate

- Geolocation
- Knowledge based
- Client side certificates
- Grid cards
- Out of band
- One time password systems
- PKI based systems
- Virtual keyboards
- Key stroke biometrics
- Graphical password systems
- Password managers
- Voice, facial,…
- Federated systems
- SQRL-Secure, Quick, Reliable Login

Overview 2 Factor Methods

SMS OTP

- Cost (user and issuer)
- Coverage issues
- Delay

OTP App/ Soft Certificates

- Vulnerable to malware on host system
- No 2nd factor if phone/tablet is used for Internet access

OTP fobs

- Use proprietary algorithms
- Typically one per site
- On the large side

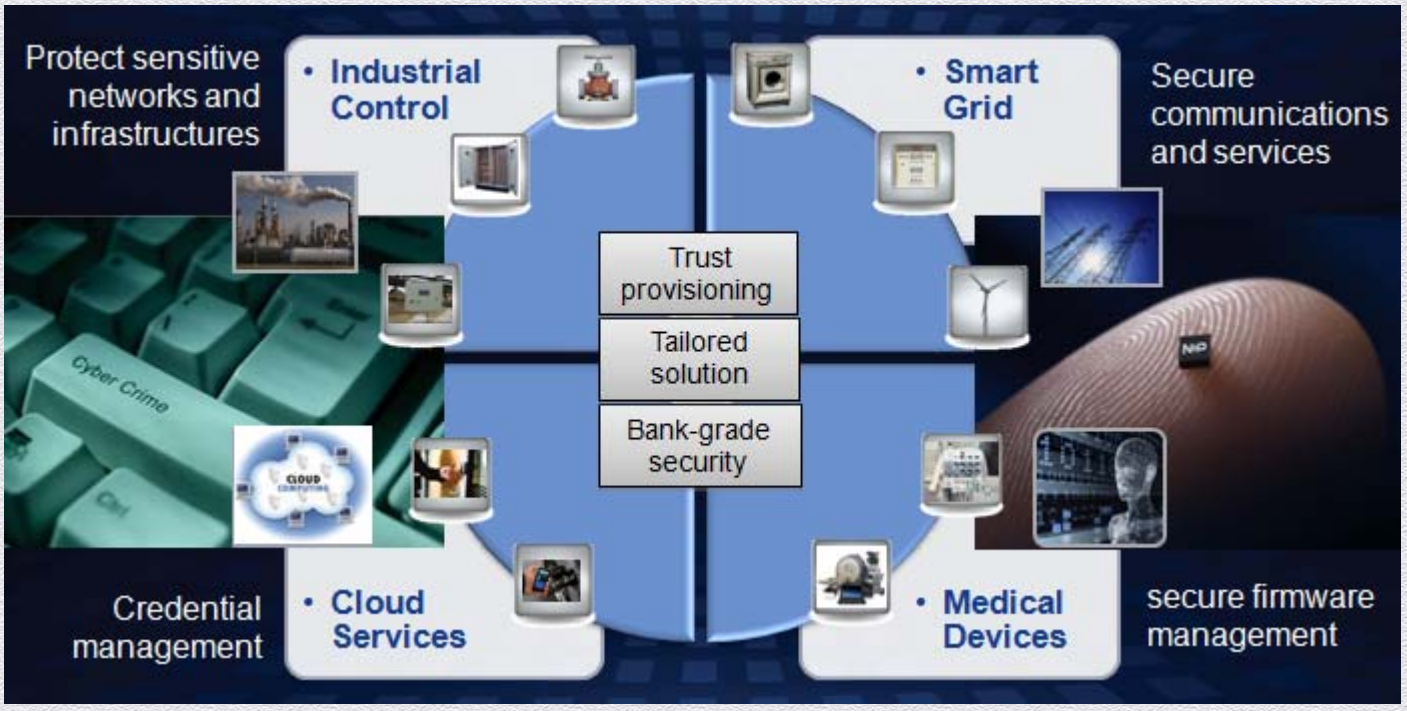
OTP Security

- Phishable
- Vulnverable to MITM and MITB attacks
- OTP not calculated in a Secure Element

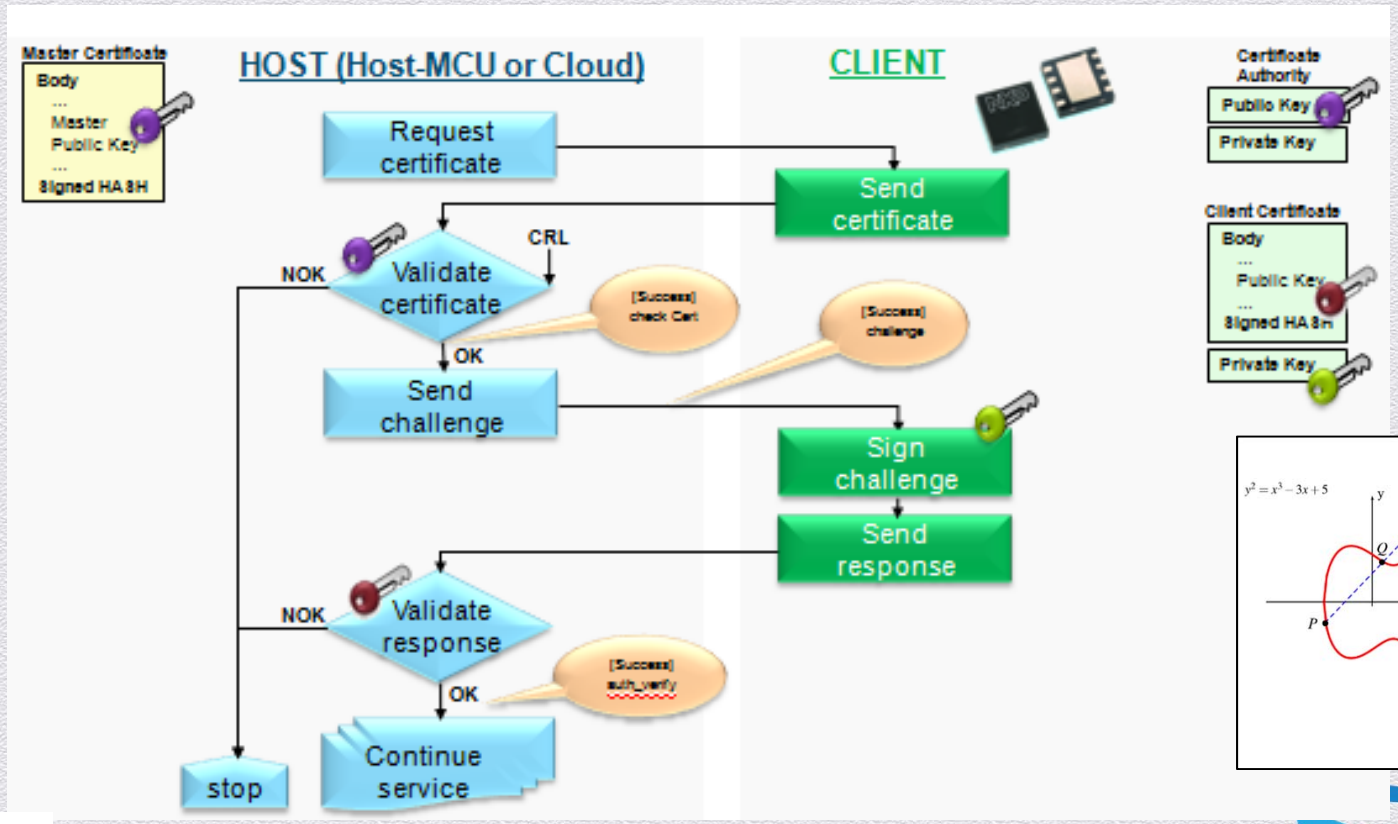
Convenience/ Features

- Type 6 or 8 digits into the phone
- Cannot hold identity
- No contactless interface

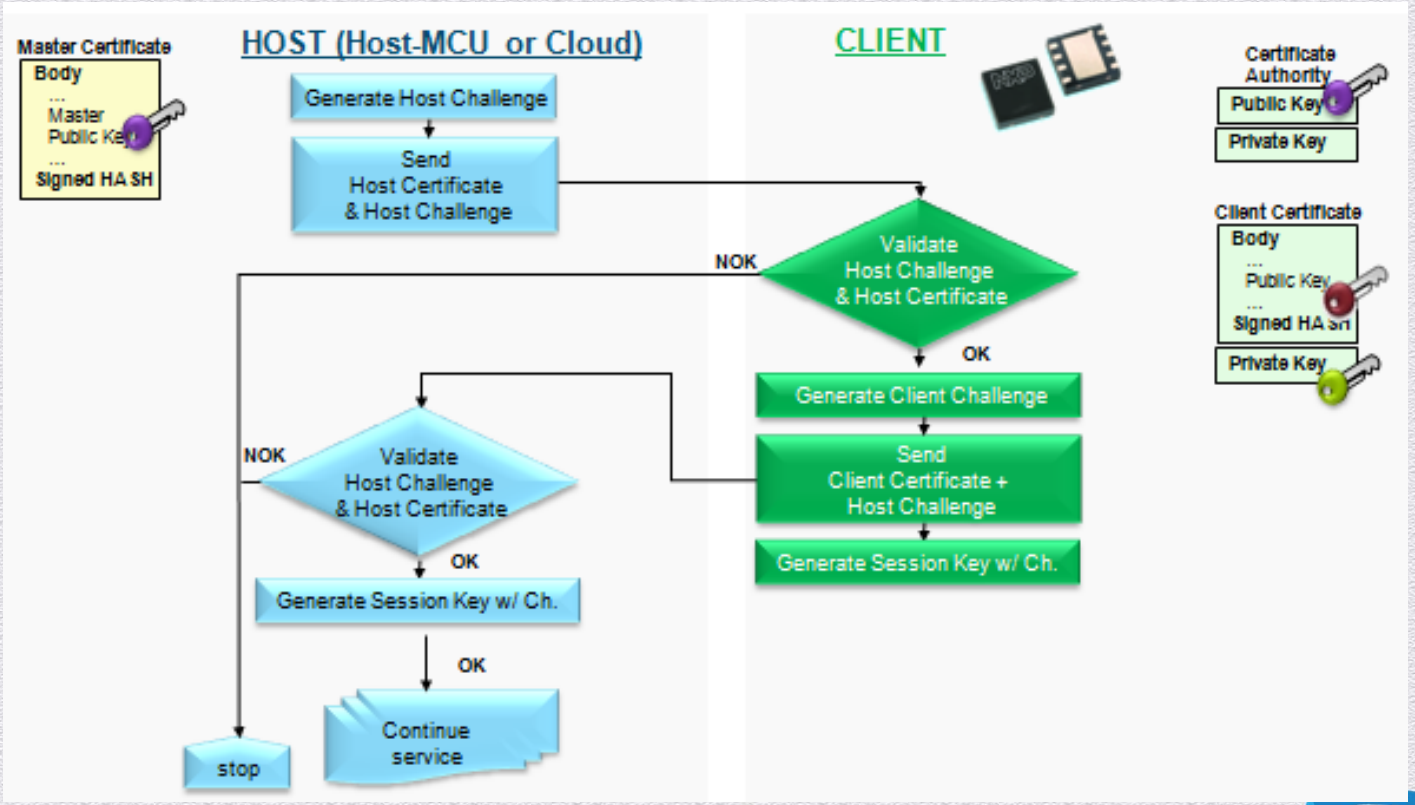
User vs. Device Authentication



Client Authentication Protocol

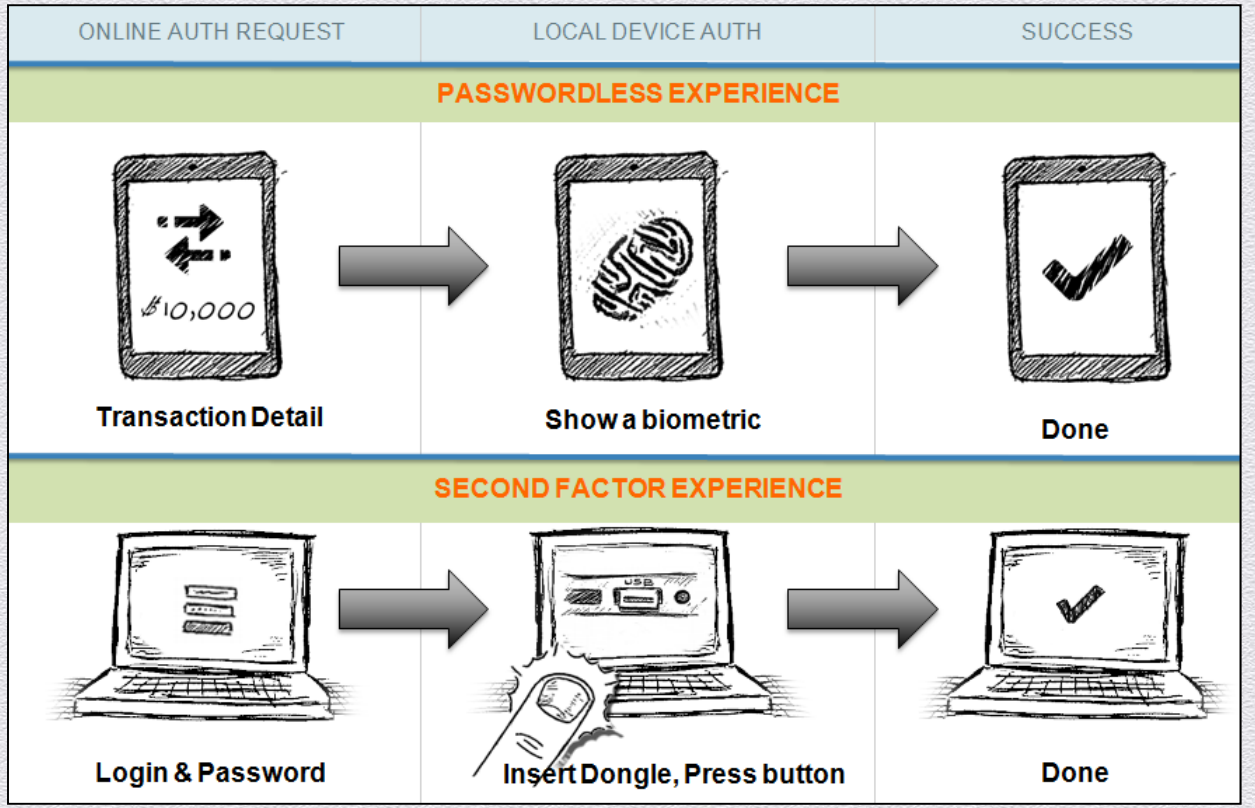


Mutual Authentication Protocol and Key Exchange

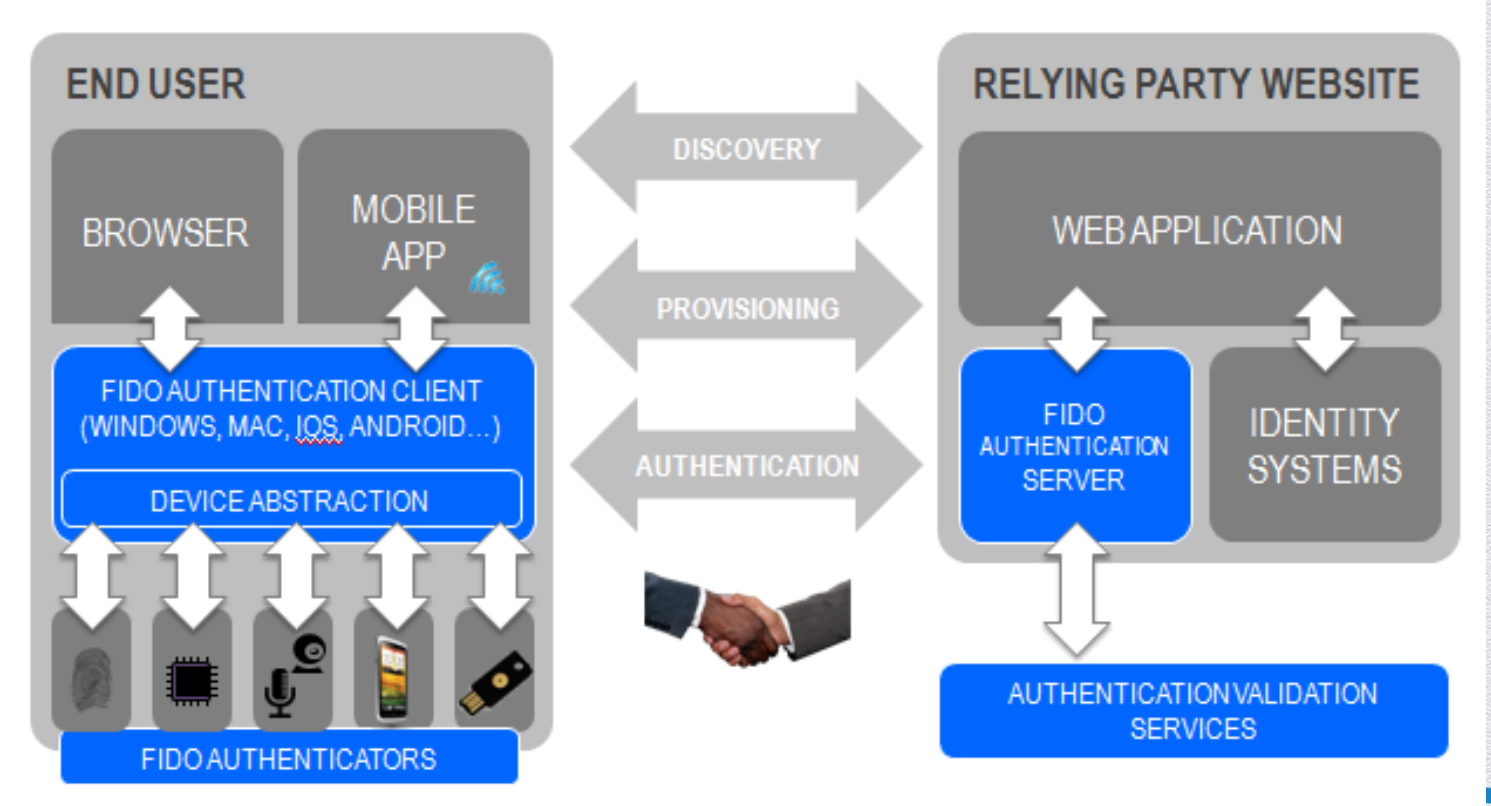


FIDO Alliance has reached critical mass

FIDO is promoting two authentication protocols



FIDO System Architecture



Useful stuff (own opinion)

- Still use a good Pa$$phr@se#1
- Use Open Source (Linux, FF, GPG, Tor, BM, Tails/Qubes, Mumble,…)
- Add-ons: NoScript, WOT, HTTPS Everywhere, …
- Leave your cell phone on and at home
- Updates (OS, Browser, Sumatra PDF, AV, Router)
- Check for open ports (https://www.grc.com/x/ne.dll?bh0bkyd2)
- Play with crypto: http://www.cryptool.org/en/

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Thank you very much

Security Basics

Sponsored by: CDNetworks

Start Time	Title	Presenter
8:30 AM	Introduction	Hugh Thompson
8:45 AM	Security Industry and Trends	Hugh Thompson
9:30 AM	Authentication Technologies	Michael Poitner
10:15 AM	Break	
10:30 AM	Governance, Risk and Compliance	Dennis Moreau
11:15 AM	Application Security	Jason Brvenik
12:00 PM	Lunch	
1:15 PM	Crypto 101/Encryption Basics, SSL & Certificates	Benjamin Jun
2:00 PM	Firewalls and Perimeter Protection	Dana Wolf
2:45 PM	Break	
3:00 PM	Viruses, Malware and Threats	Tas Giakouminakis
3:45 PM	Mobile and Network Security	Mike Janke

RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Crypto 101/Encryption, SSL & Certificates

SESSION ID: SEM-MO1

Benjamin Jun

Vice President and Chief Technology Officer
Cryptography Research, a division of Rambus

Slides adapted from: Ivan Ristic, Qualys (RSAC 2011)

Agenda

CRYPTOGRAPHY

VULNERABILITIES

SSL / TLS

CERTIFICATES

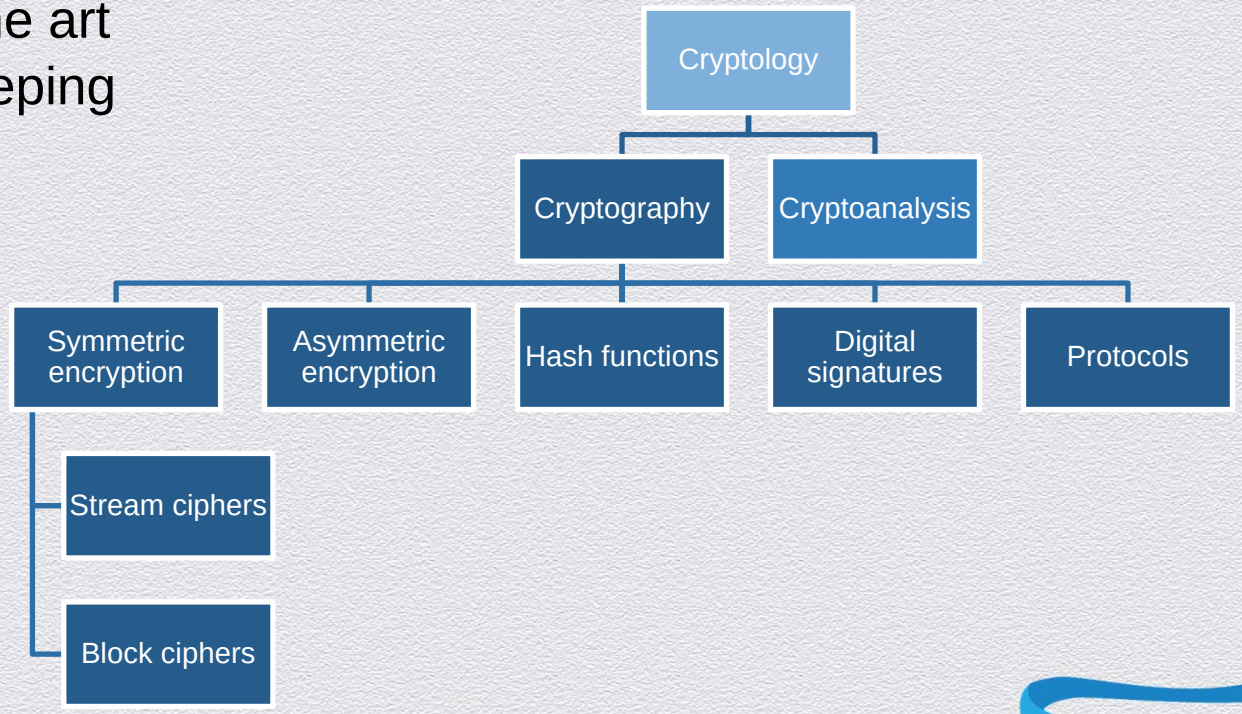
RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

CRYPTOGRAPHY

What is Cryptography?

Cryptography is the art and science of keeping messages secure.



What Does Secure Mean?

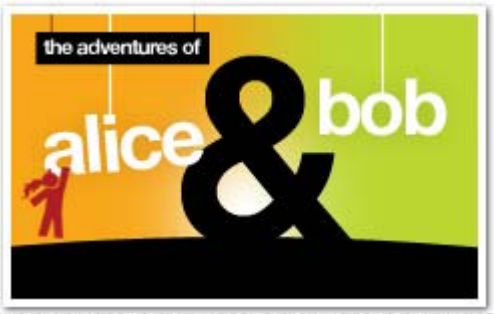
Always required:

- Confidentiality
- Integrity
- Authentication
- Non-repudiation

Other criteria:

- Interoperability
- Performance

Meet Alice and Bob



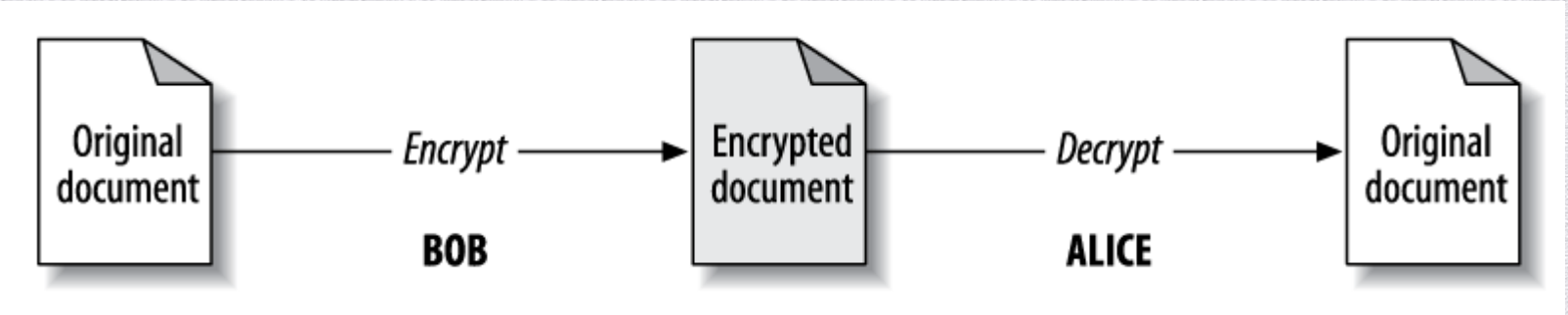
Good guys:

- Alice, Bob

Bad guys:

- Eve (passive, eavesdropped)
- Mallory, Oscar, Trudy (active, man in the middle)

Restricted Versus Open



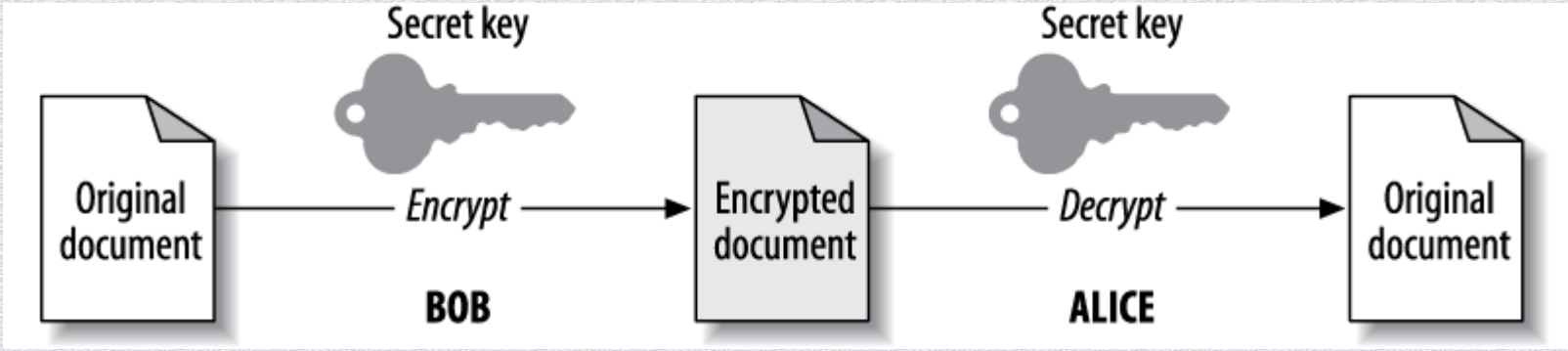
Issues:

- Need different algorithm for every communication group
- Algorithms must be thrown away on compromise, or when someone leaves group
- *Difficult to validate algorithms are secure*

How Does Encryption Work?

- Obfuscation that is fast when you know the secrets, but impossible or slow when you don't.
- *Computational security* means that something cannot be broken with available resources, either now or in the future.
- Aspects of complexity:
  - Amount of data
  - Processing power
  - Memory capacity

Symmetric Encryption



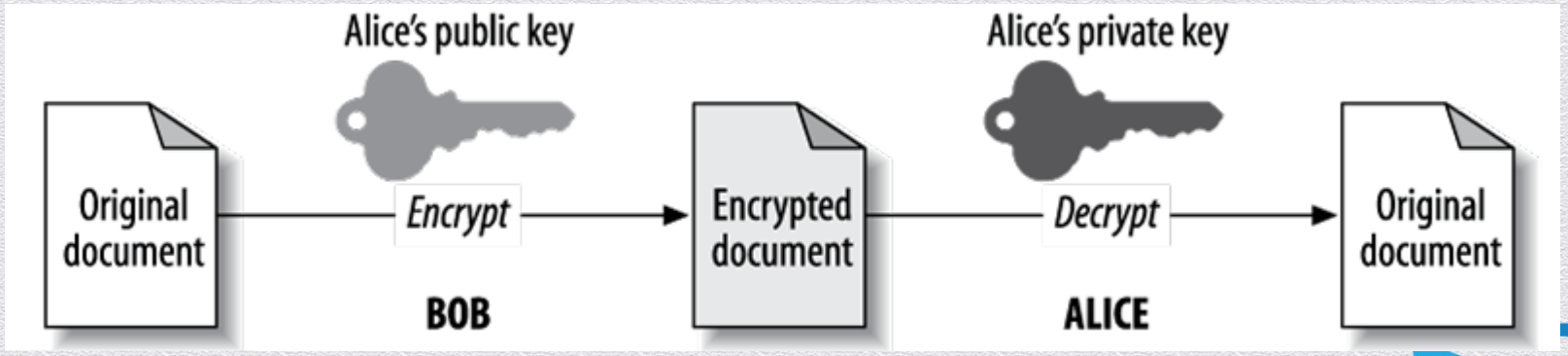
Convenient and fast:

- Common algorithms: RC4, 3DES, AES
- Secret key must be agreed on in advance
- Group communication requires secure key distribution
- No authentication

Asymmetric Encryption

Asymmetric encryption uses two keys; one private and one public. The keys are related.

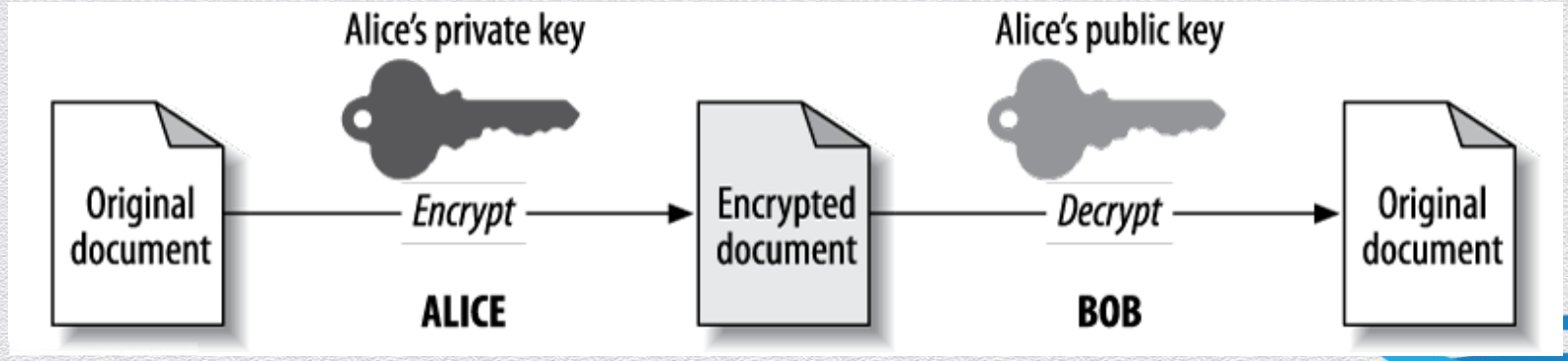
- RSA, Diffie-Hellman key exchange, Elgamal encryption, and DSA. Also ECDH and ECDSA.
- Enables authentication and secure key exchange.
- Significantly slower than symmetric encryption.



Digital Signatures

Well-known algorithms:

- RSA
  - Textbook approach – just encrypt with private key
  - In practice, use digest and strengthen
- DSA, ECDSA



Random Number Generation

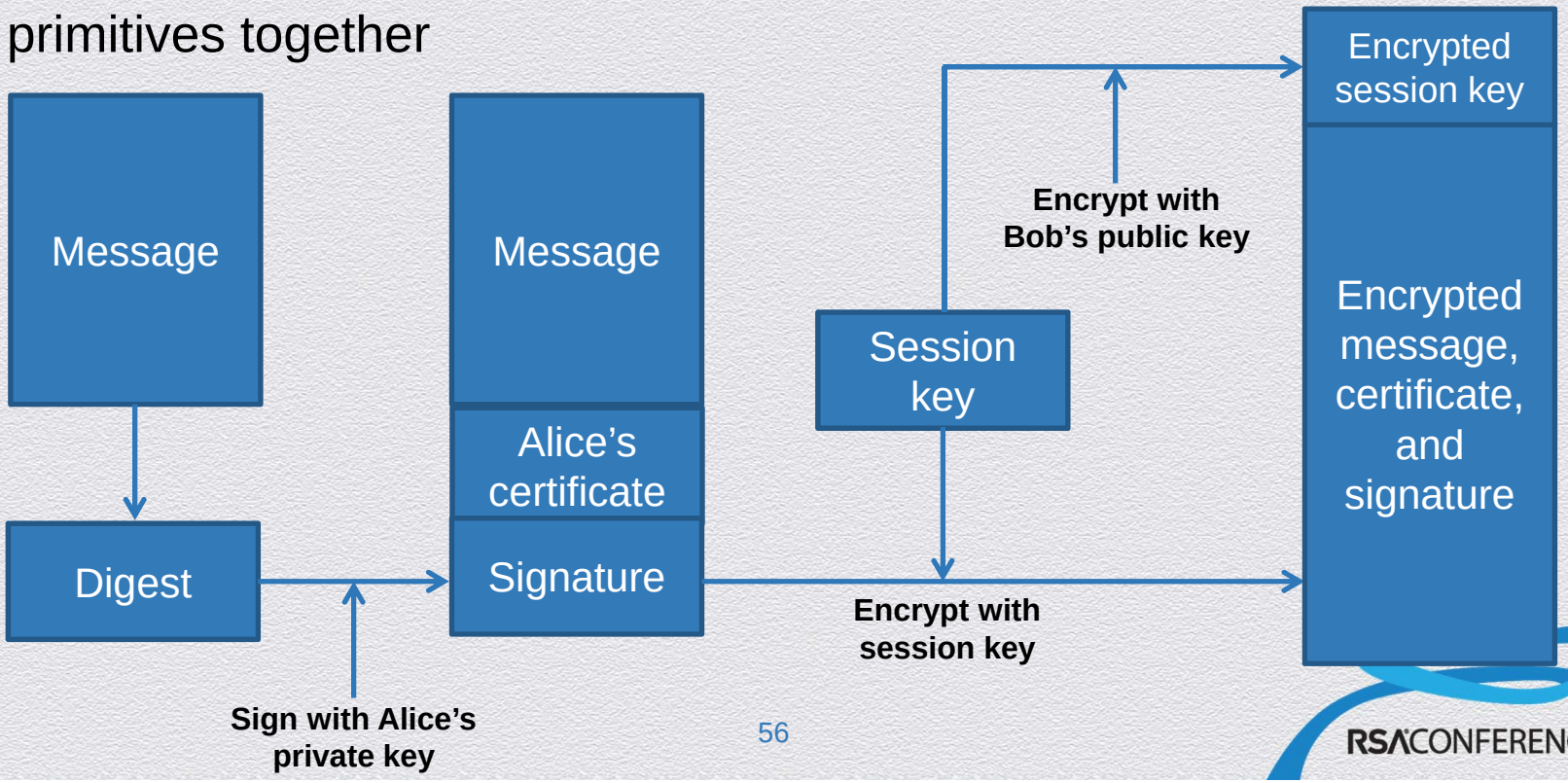
- Random numbers are at the heart of cryptography.
  - Used for key generation
  - Weak keys equal weak encryption
- Types of random number generators:
  - True random number generators (TRNG) – *truly random*
  - Pseudorandom number generators (PRNG) – *look random*
  - Cryptographically secure pseudorandom number generators (CSPRNG) – *look random and are unpredictable*

Hash Functions

- Hash functions are lossy one-way transformations that result with fixed-length *data fingerprints*. Usually used for:
  - Digital signatures
  - Integrity validation
  - Tokenization (e.g., storing passwords)
- Desirable qualities of hash functions:
  - Preimage resistance (one-wayness)
  - Weak collision resistance (2nd preimage resistance)
  - Strong collision resistance and the Birthday attack

Protocols

- Communicating securely requires more effort than just putting the primitives together

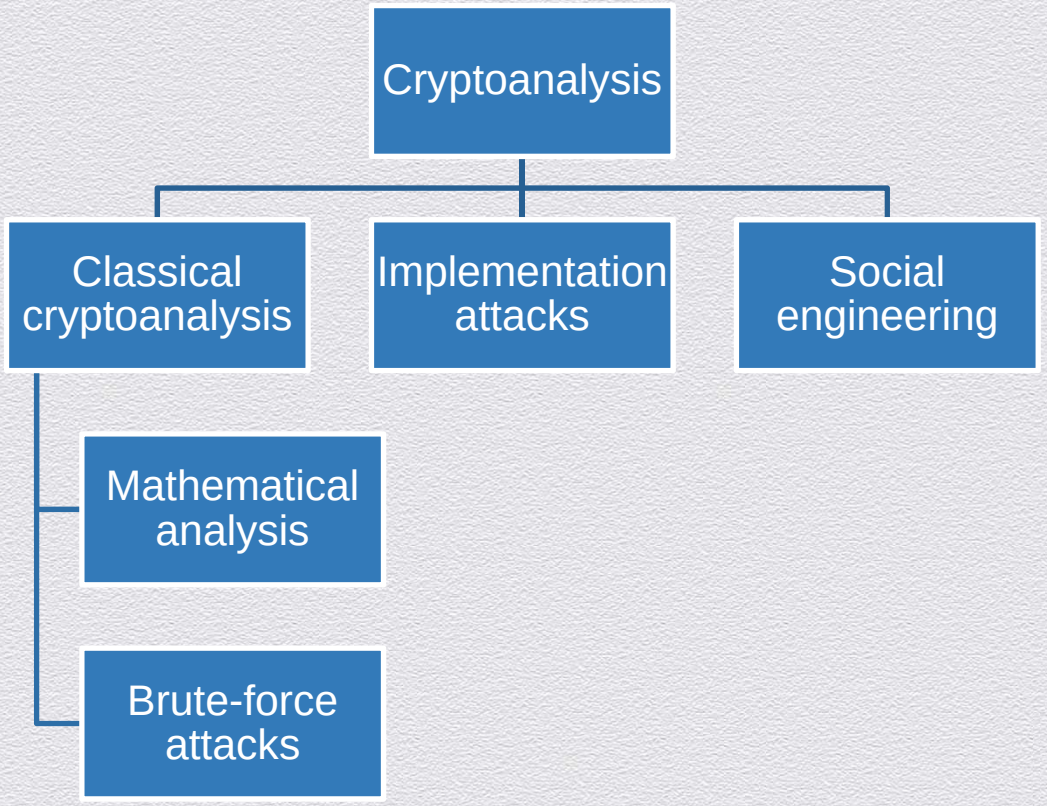


RSA CONFERENCE 2014

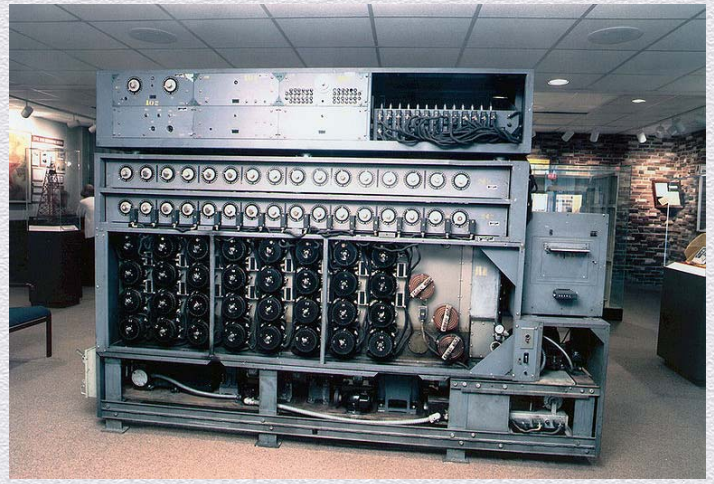
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

VULNERABILITIES

Attacks on Cryptography



Example: Brute Force (Cryptanalysis)



US Navy Bombe, 1943

Contains 16 four-rotor Enigma equivalents to perform exhaustive key search.

DES Keysearch Machine, 1998 (Cryptography Research, AWT, EFF)

Tests over 90 billion keys per second, taking an average of less than 5 days to discover a DES key.

CRYPTOGRAPHY RESEARCH
a division of Rambus

Example: Side-Channel (Implementation)

- Simple EM attack with a radio
- Usable signals even at 10 feet away

Devices

far field

near field

Antennas

Digitizer,
GNU Radio peripheral
($1000)

Receiver ($350)

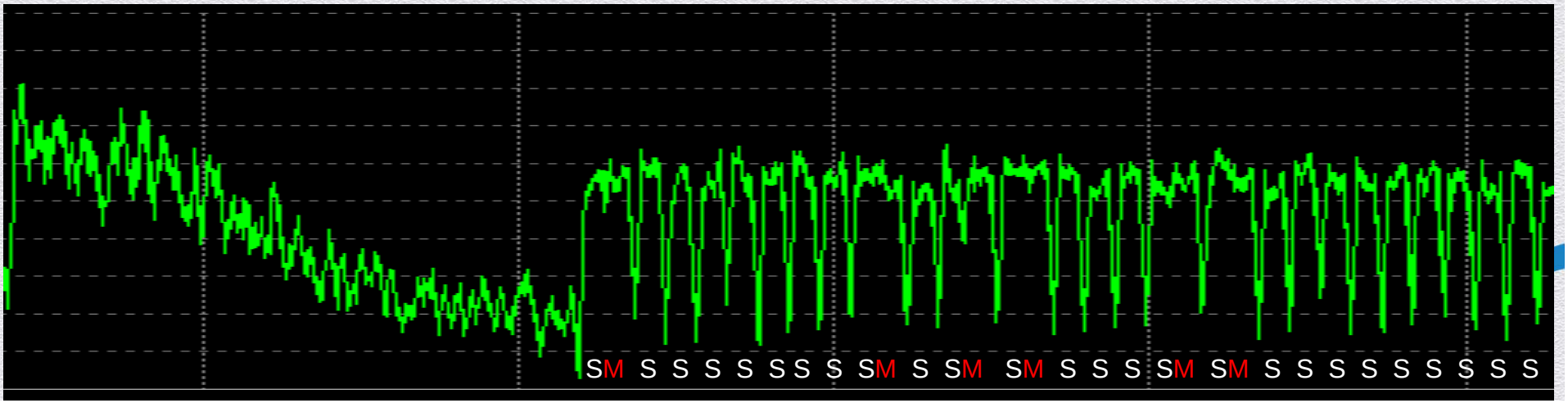
Signal Processing
(demodulation, filtering)

DPAWS™ side-channel
analysis software

Example: Side-Channel (Implementation)

- Focus on Mp^{dp} mod p calculation (Mq^{dq} mod q similar)

```
For each bit i of secret dp
   perform "Square"
   if (bit i == 1)
     perform "Multiply"
   endif
endfor
```



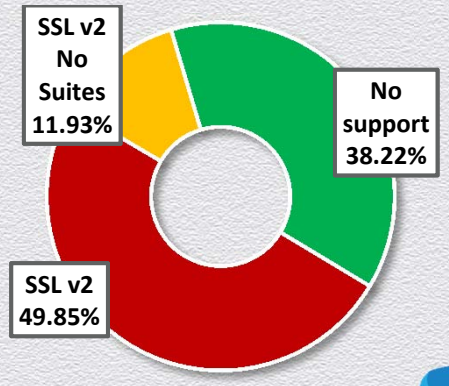
RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

SSL/TLS

Introduction to SSL

- SSL is a hybrid protocol designed to turn an insecure communication channel (regardless of protocol) into a secure one
- Designed by Netscape in 1994, standardized in 1999 as TLS, which is now at version 1.2 (2008)
- Protocol versions so far:
  - SSL v2 – insecure
  - SSL v3 – still secure, but lacking
  - TLS v1 – widely used, but not best
  - TLS v1.1, v1.2 – not widely used



SSL Goals

- The SSL standard packages our knowledge of security protocols for resuse
- Key services:
  - Discovery and authentication
  - Session key(s) generation
  - Communication integrity
  - Interoperability
  - Extensibility
  - Performance

SSL Cipher Suites

- SSL cipher suites are a higher-level cryptographic construct, consisting of:
  - Key exchange and authentication
  - Symmetric session cipher
  - Message integrity algorithm
- Examples:
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
  - TLS_RSA_WITH_RC4_128_SHA

State of SSL

- The situation is good, overall
- But there are several issues:
  - Problems with certificate authorities
  - Browsers talk to the sites with broken certificates
  - We're not good at keeping up with protocol evolution: SSL v2 still widely supported; TLS v1.1 and TLS v1.2 virtually not supported
  - Lack of support for virtual SSL in Windows XP
  - Too many plain-text (HTTP) web sites
  - Issues related to mixed content (HTTP/HTTPS)

RSA CONFERENCE 2014

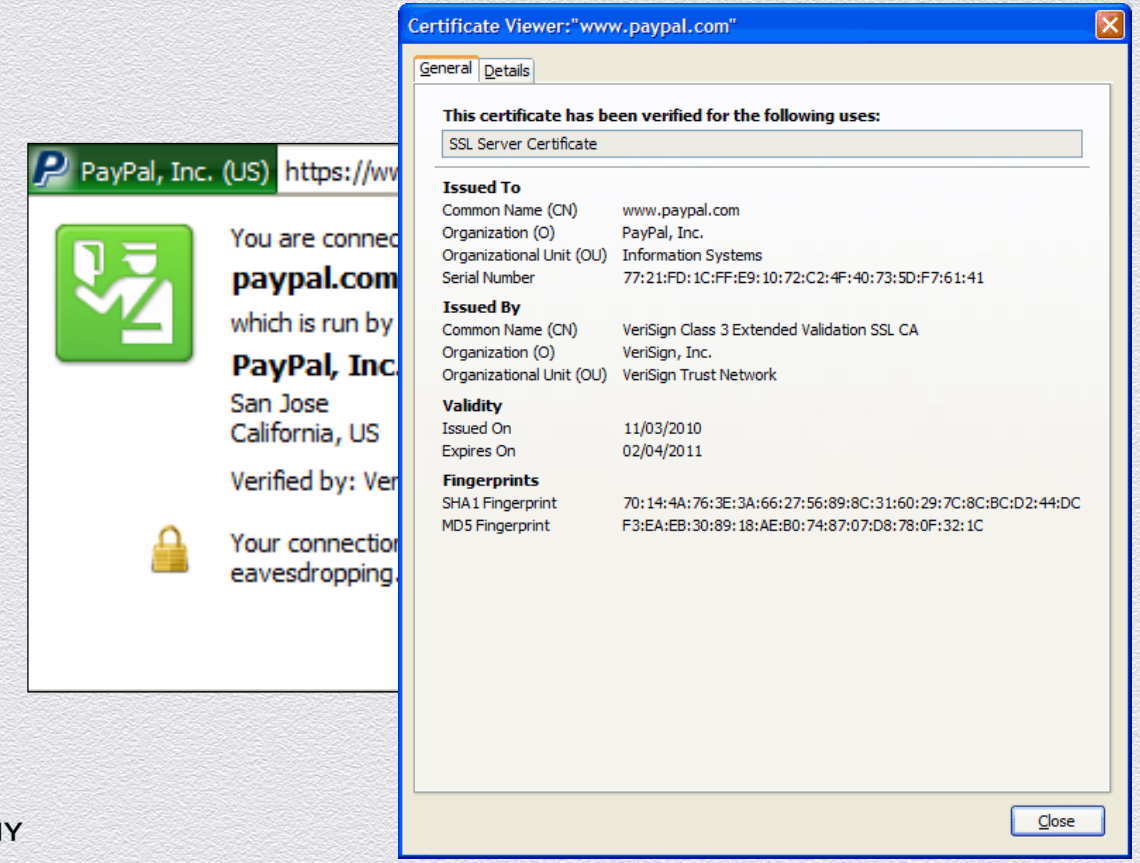
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

CERTIFICATES

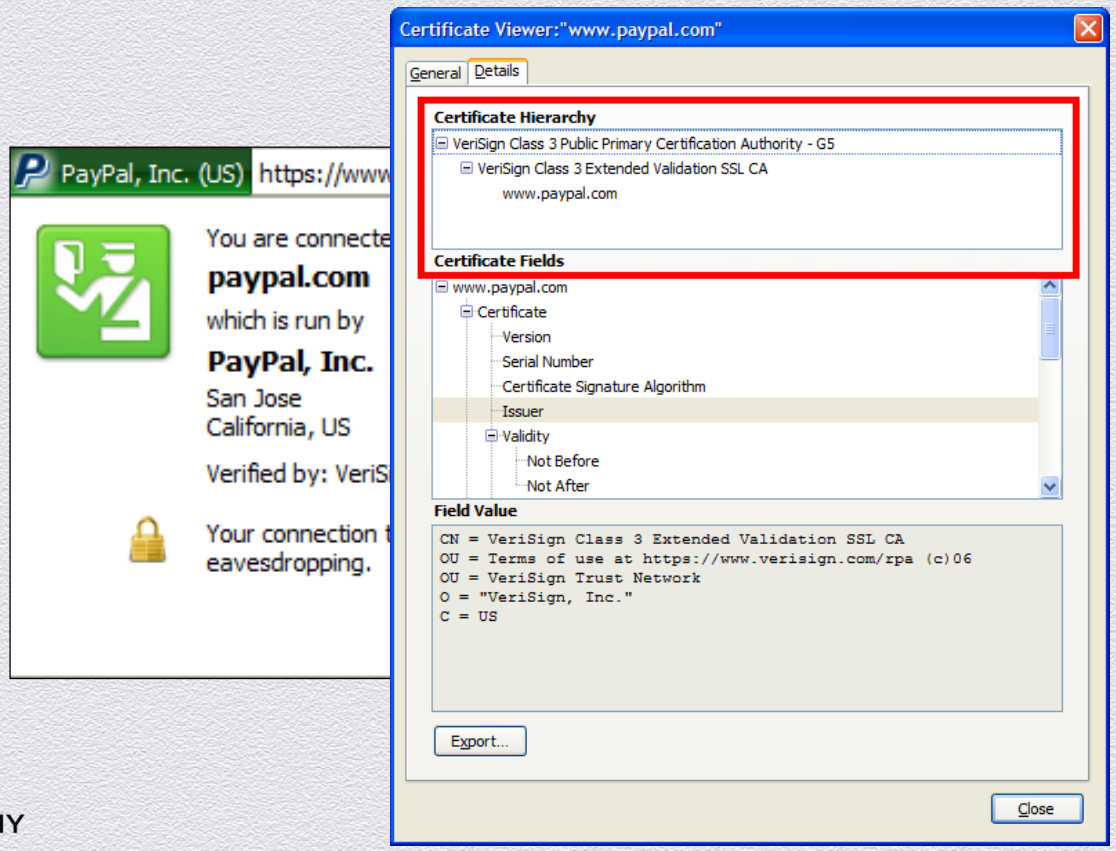
Digital Certificates

- Digital identity often include a public/private keypair
  - Usually exchanged at start of a session
  - It is necessary to authenticate the keypair when faced with an active man-in-the-middle attack
- We need third parties to help establish identity – generally a *certificate authority (CA)*
- Digital certificates contain a public key, some identifying information (e.g., name, address, etc.) and a signature

Certificate Contents



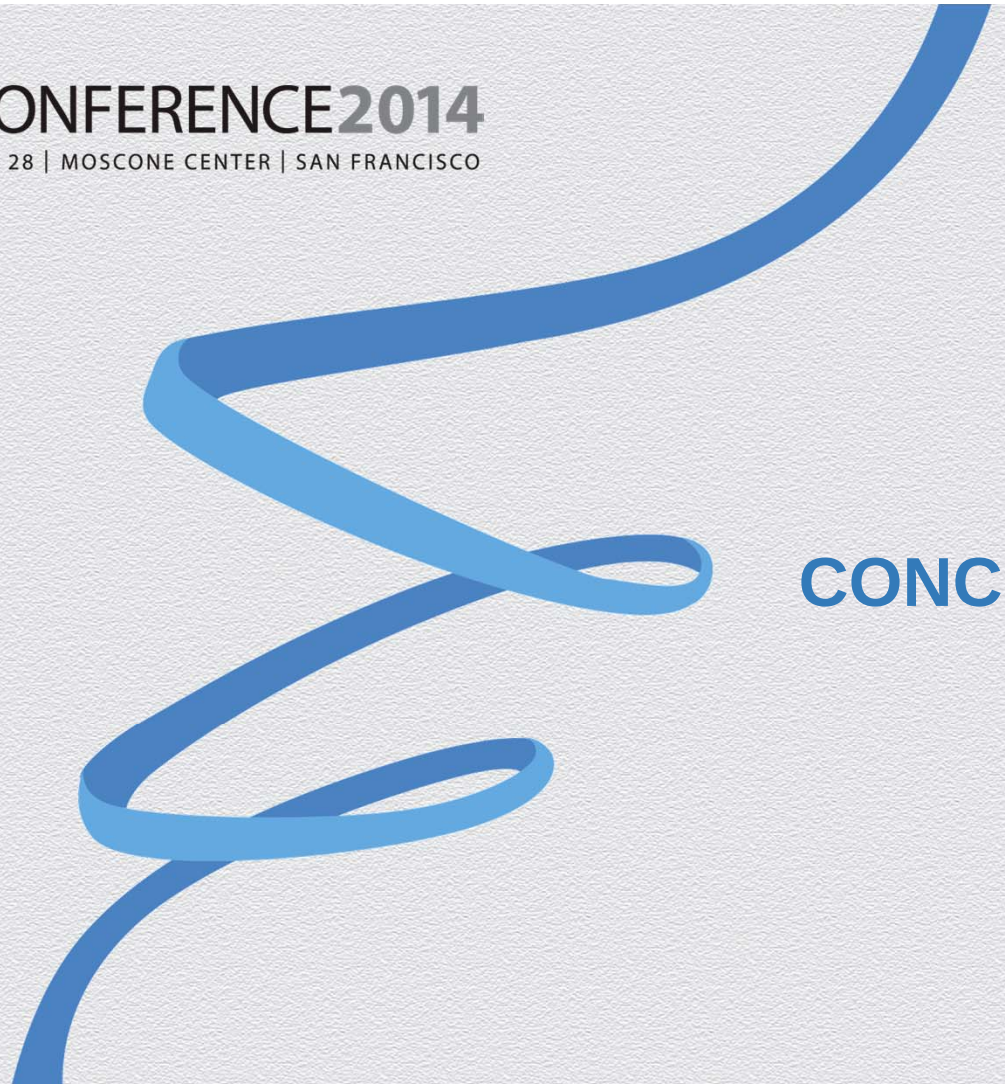
Certificate Chaining



Certificate Authorities

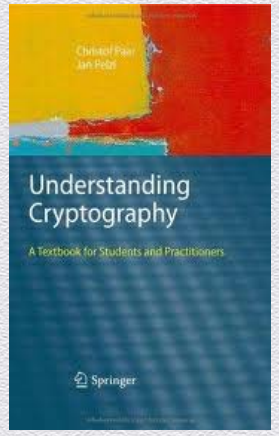
- Estimated ~ 650 certificate authorities (EFF)
  - Most browsers trust a small (ish) number of root certs, but the overall number grows through chaining
- Any CA can issue certificate for any site
- Strong desire to keep certificates in DNS (not that we are starting to implement DNSSEC)

The EFF SSL Observatory
https://www.eff.org/observatory

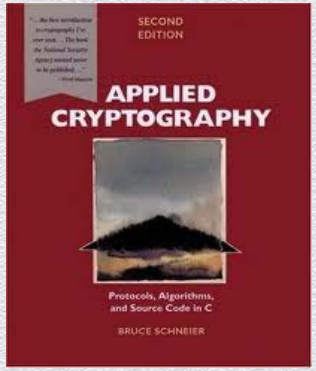


CONCLUSIONS

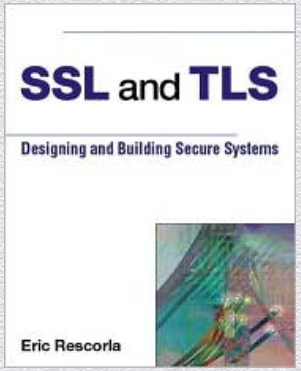
Resources



Understanding Cryptography
Christof Paar and Jan Pelzl
(Springer, 2009)



Applied Cryptography
Second Edition
Bruce Schneier
(Wiley, 1996)



SSL and TLS
Eric Rescorla
(Addison Wesley, 2001)

SSL Labs
www.ssllabs.com
Qualys

How to Apply What You Have Learned

- In the first three months, you should:
  - Identify where cryptography is used in your organization
  - Identify infrastructure required for cryptography implementations (key management, certificates)
- Within six months, you should:
  - Know what crypto **can** do. Explain the different security properties.
  - Know what crypto **can't** do. Gain basic knowledge of implementation security issues.

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

QUESTIONS?

Security Basics

Sponsored by: CDNetworks

Start Time	Title	Presenter
8:30 AM	Introduction	Hugh Thompson
8:45 AM	Security Industry and Trends	Hugh Thompson
9:30 AM	Authentication Technologies	Michael Poitner
10:15 AM	BREAK	
10:30 AM	Governance, Risk and Compliance	Dennis Moreau
11:15 AM	Application Security	Jason Brvenik
12:00 PM	LUNCH	
1:15 PM	Crypto 101/Encryption Basics, SSL & Certificates	Benjamin Jun
2:00 PM	Firewalls and Perimeter Protection	Dana Wolf
2:45 PM	Break	
3:00 PM	Viruses, Malware and Threats	Tas Giakouminakis
3:45 PM	Mobile and Network Security	Mike Janke

RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Firewalls & Perimeter Security

SESSION ID: SEM-M01

Dana Elizabeth Wolf

Sr. Director of Products
OpenDNS
@dayowolf

Firewall & Perimeter in 45 minutes

- History of the Perimeter
- The Morris Worm
- What is a firewall?
- Packets & Protocols
- Features of a firewall
- What it protects

OpenDNS

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Quick History of the Evolution of the Perimeter

Security: Physical Enforcement

OpenDNS

Security: Access Enforcement

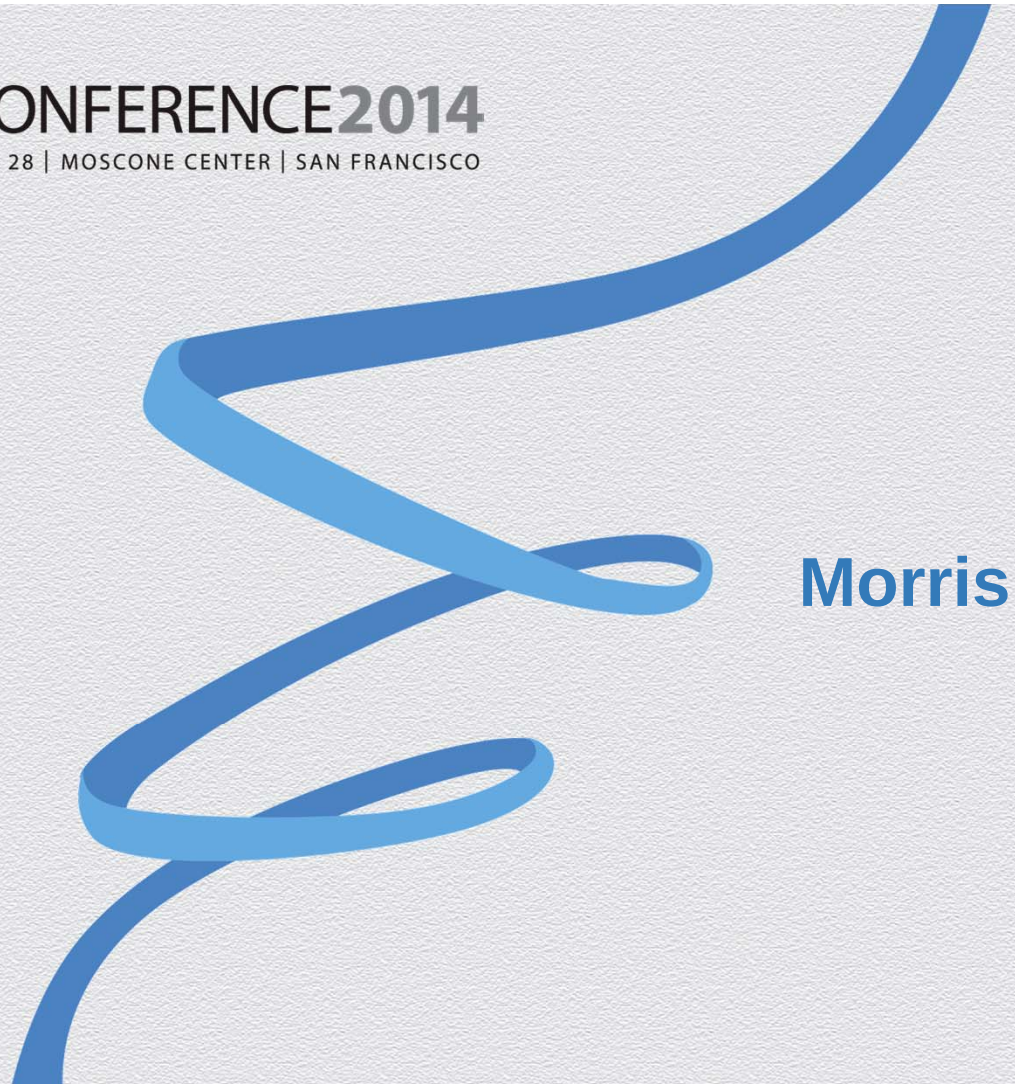
Security: Local Access/Authentication Enforcement

OpenDNS

<New Enforcement?>

OpenDNS

So WHAT is the Perimeter?



Morris Worm

The Morris Worm

- 1988, Robert Morris wrote an experimental, self-replicating, self-propagating program
- Called “a worm”
- Many machines at locations around the country crashed or became “catatonic”
- Cost of dealing with worm at each location: $200-$53,000
- Concept of “firewall” introduced

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Perimeter Security

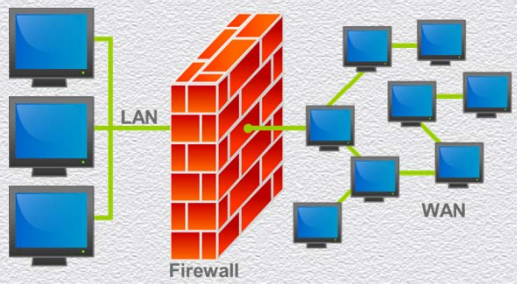
OpenDNS

Some “creative” ways attackers try to gain access

- Remote login
- Application backdoors
- SMTP session hijacking
- OS Bugs
- Denial of service
- Redirect bombs
- Email bombs
- Viruses
- Source Routing
- Port scanning

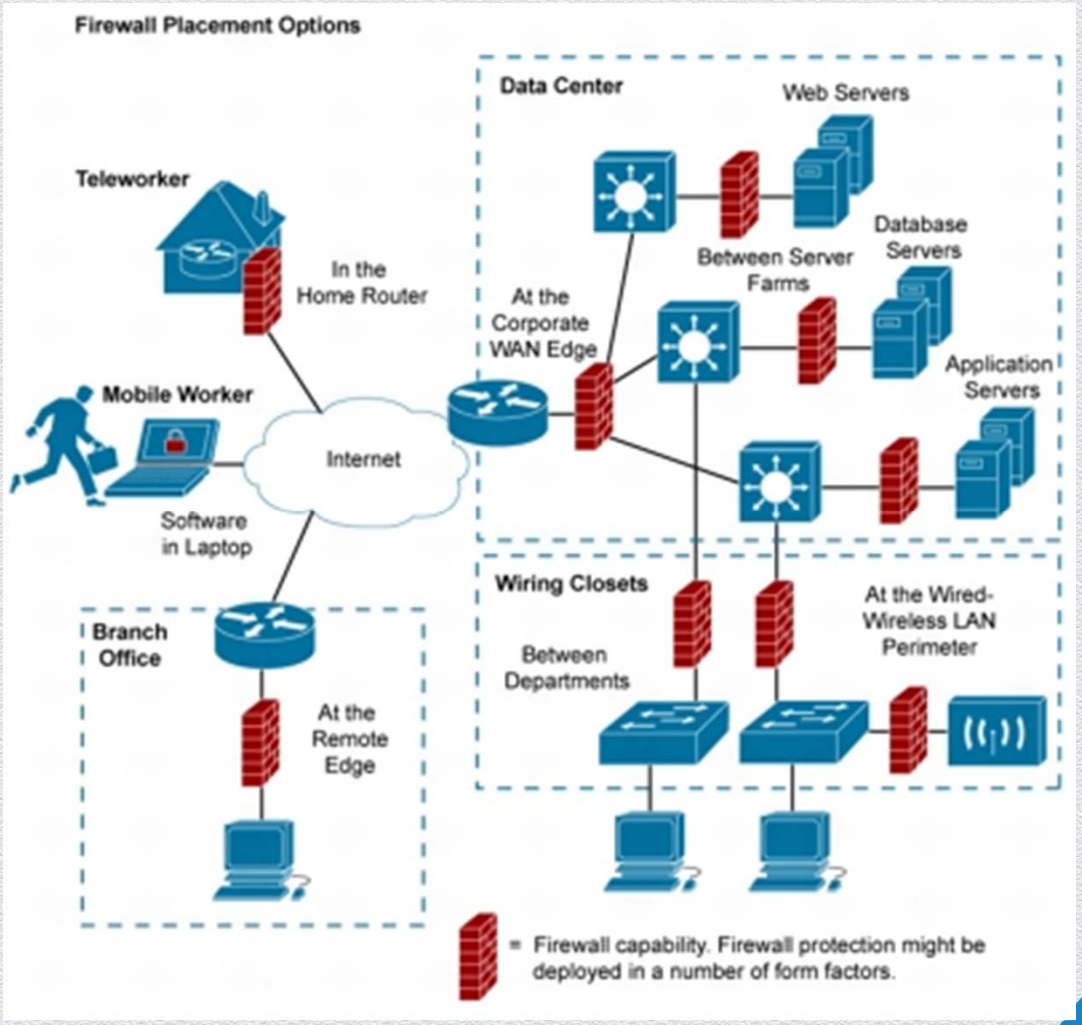
OpenDNS

Definition of a Firewall



- Prevents the dangers of the internet from spreading to your internal network
- Collection of components placed between two networks that collectively have the following properties:
  - All traffic from inside to outside (and vice versa) must pass through the firewall
  - Only authorized traffic, as defined by policy, will be allowed to pass
  - The firewall itself is immune to penetration

OpenDNS



OpenDNS

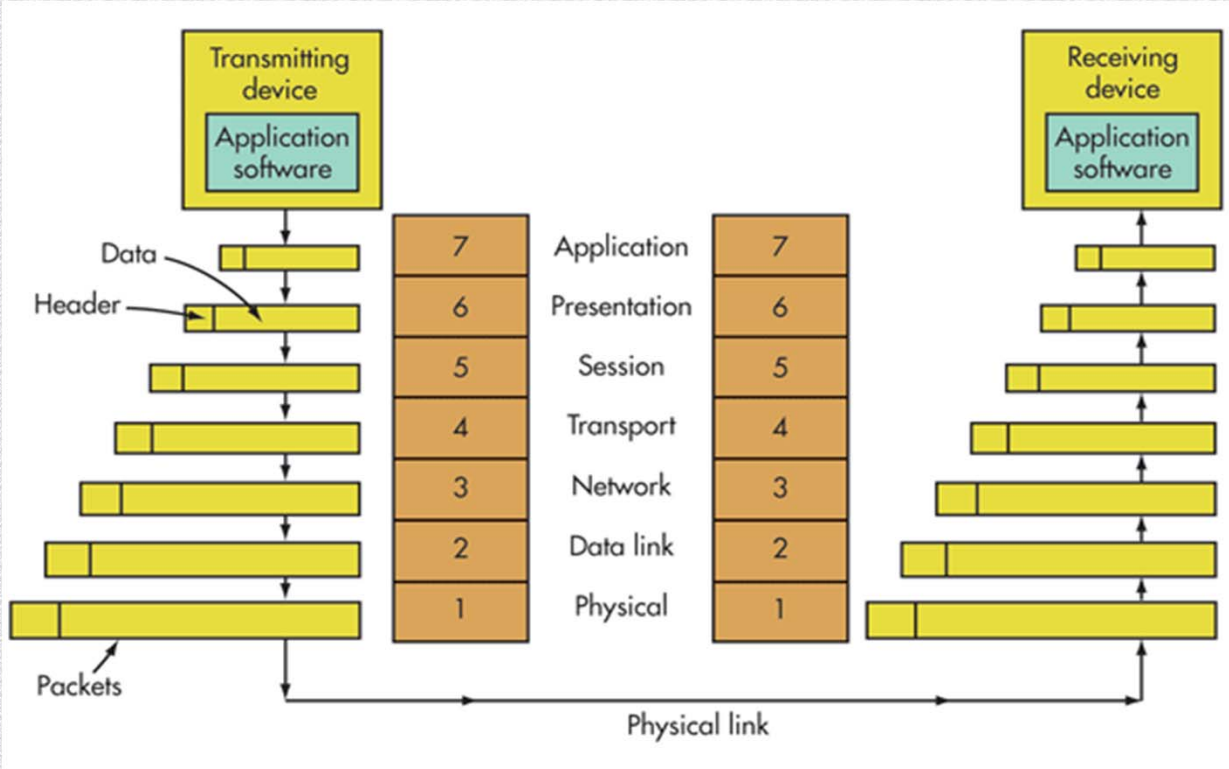
#RSAC

RSACONFERENCE2014

RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Firewall Technologies/Components

Network Protocol

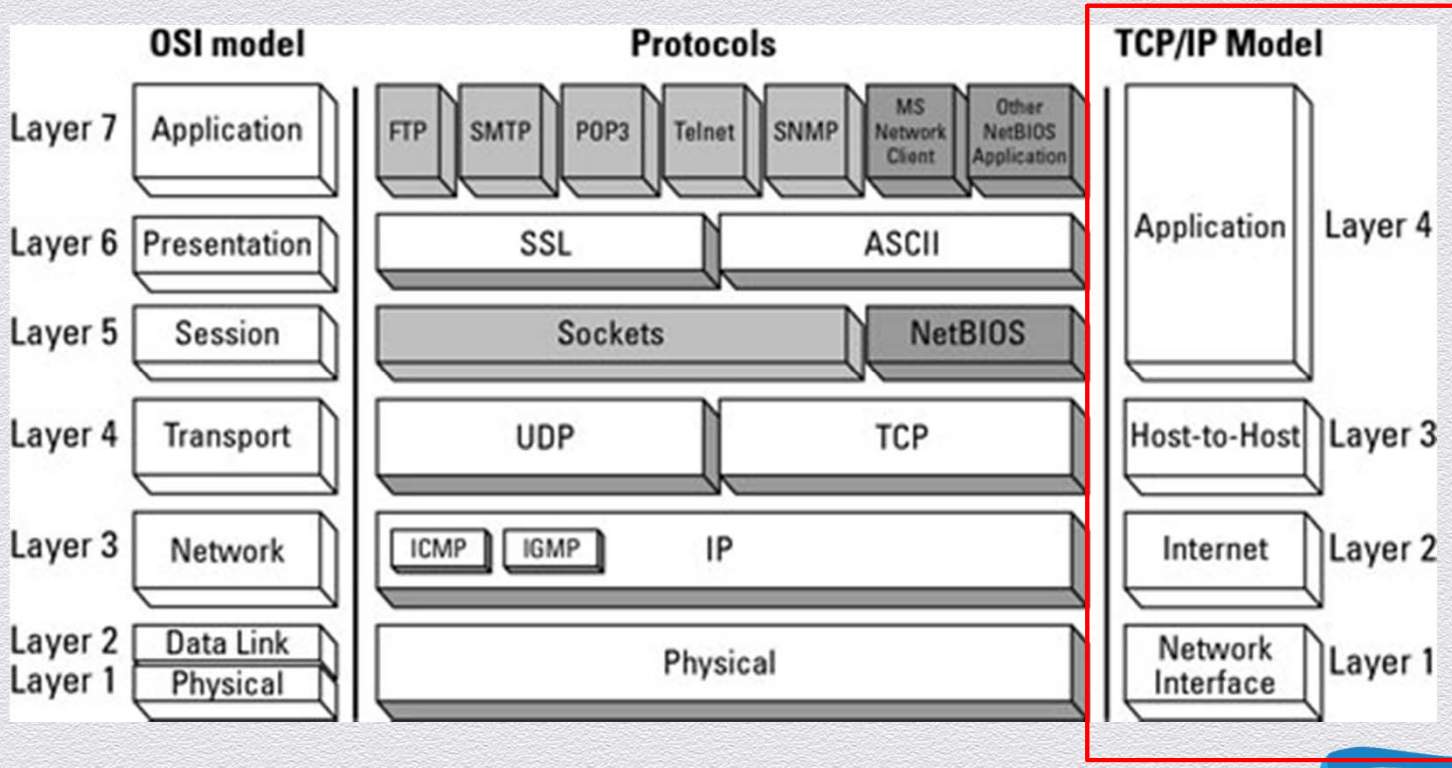


OpenDNS

#RSAC

RSACONFERENCE2014

Protocol stack

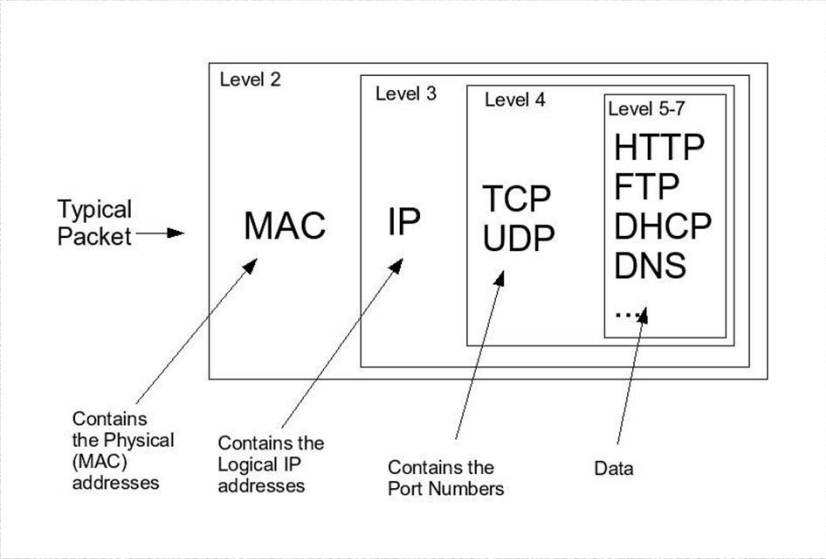


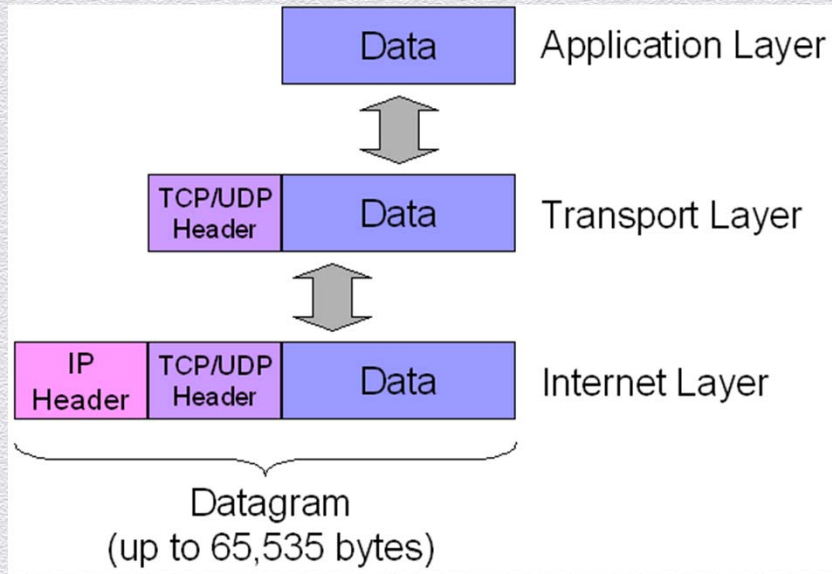
OpenDNS

#RSAC

RSACONFERENCE2014

Packet building





Packet Filtering

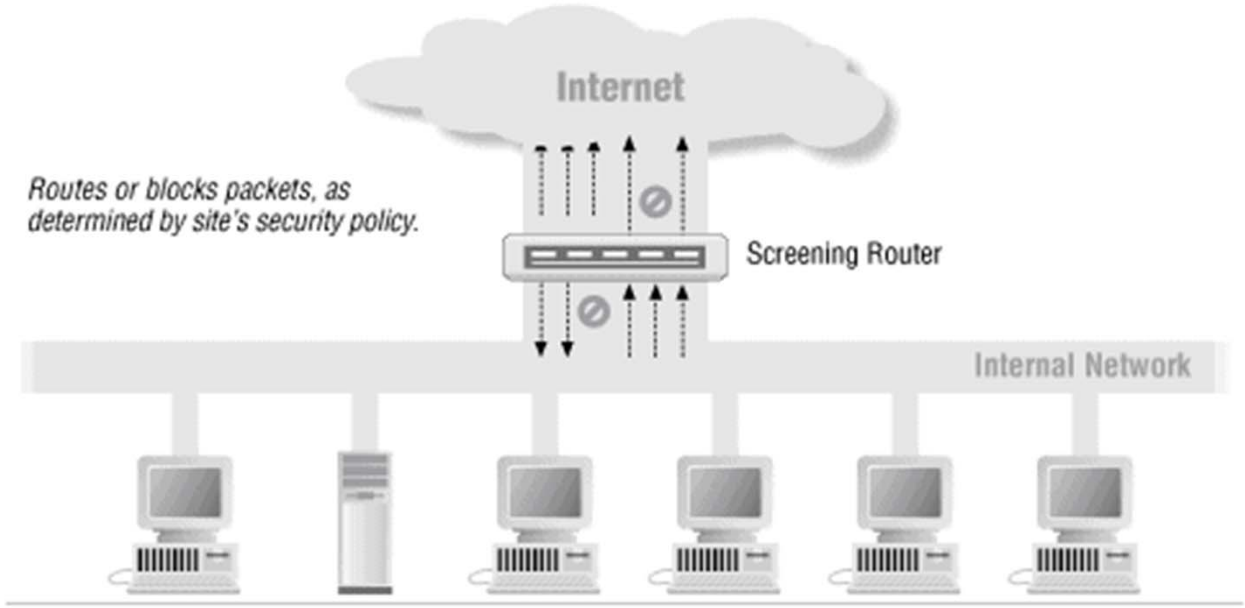


Figure 5.1. Using a screening router to do packet filtering

Packet Filtering: Advantages/Disadvantages

- Advantages
  - A single router can help protect an entire network
  - Packet filtering is widely available
  - Simple packet filtering is very efficient
- Disadvantages
  - Reduces router performance
  - Some policies cannot be easily enforced by normal packet filtering routers
  - Current tools are not perfect

Host Terminology

- Host: *Computer system attached to a network*
- Bastion Host: *Special purpose computer specifically designed & configured to withstand attacks*
- Dual-homed host: *System fitted with at least 2 NICs that sits between a trusted & untrusted network*

Proxy Services

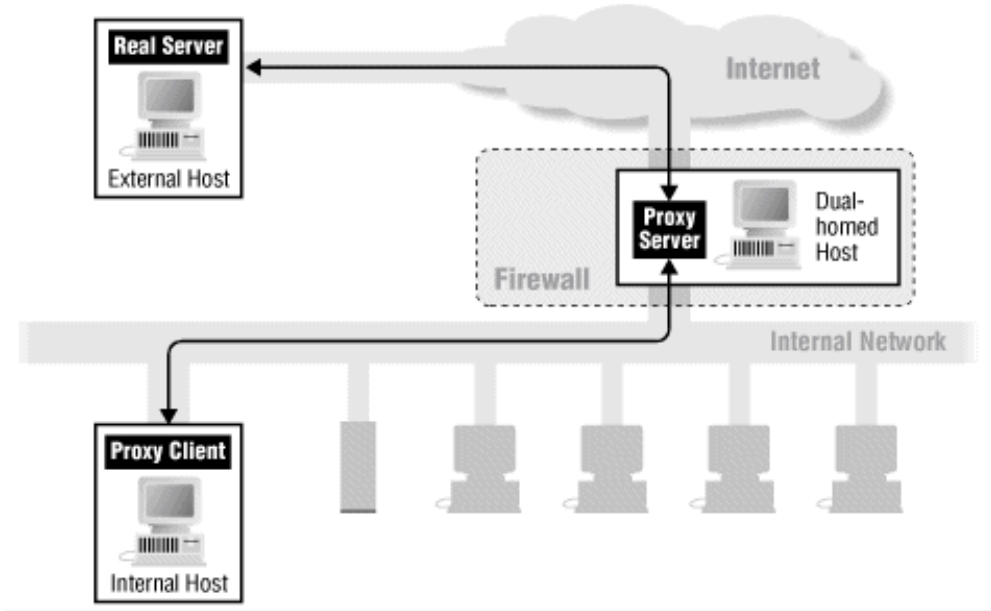


Figure 5.2. Using proxy services with a dual-homed host

Proxying: Advantages/Disadvantages

- Advantages
  - Can be good at logging
  - Can provide caching & intelligent filtering
  - Can perform user-level authentication
  - Provide protection for weak or faulty IP implementations
- Disadvantages
  - Lag behind non-proxied services
  - Require modifications to clients, applications or procedures

Network Address Translation

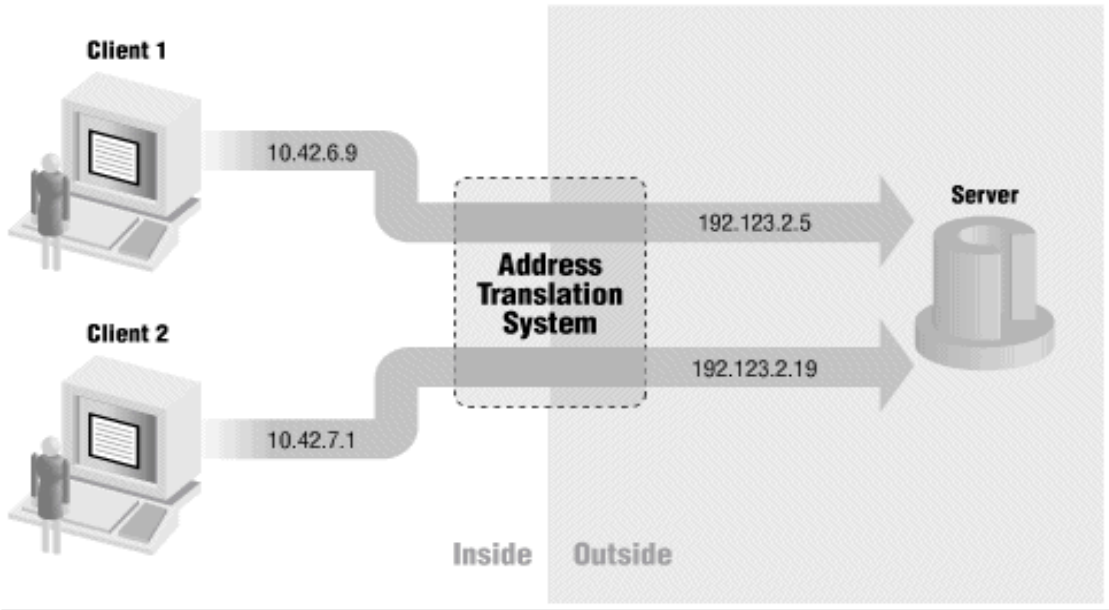


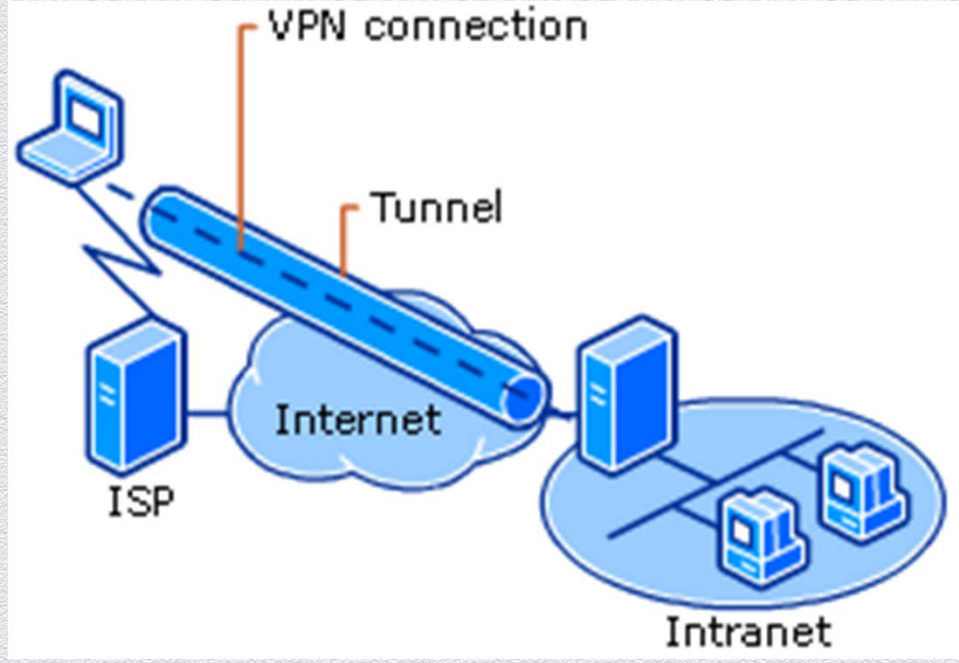
Figure 5.3. Network address translation

NAT: Advantages/Disadvantages

- Advantages
  - Helps enforce the firewalls control over outbound connections
  - Can help restrict incoming traffic
  - Conceals the internal network's configuration
- Disadvantages
  - Requires state information that isn't always available
  - Interferes with some encryption and authentication systems
  - Has a problem with Embedded IP addresses
  - Dynamic allocation may interfere with packet filtering

OpenDNS

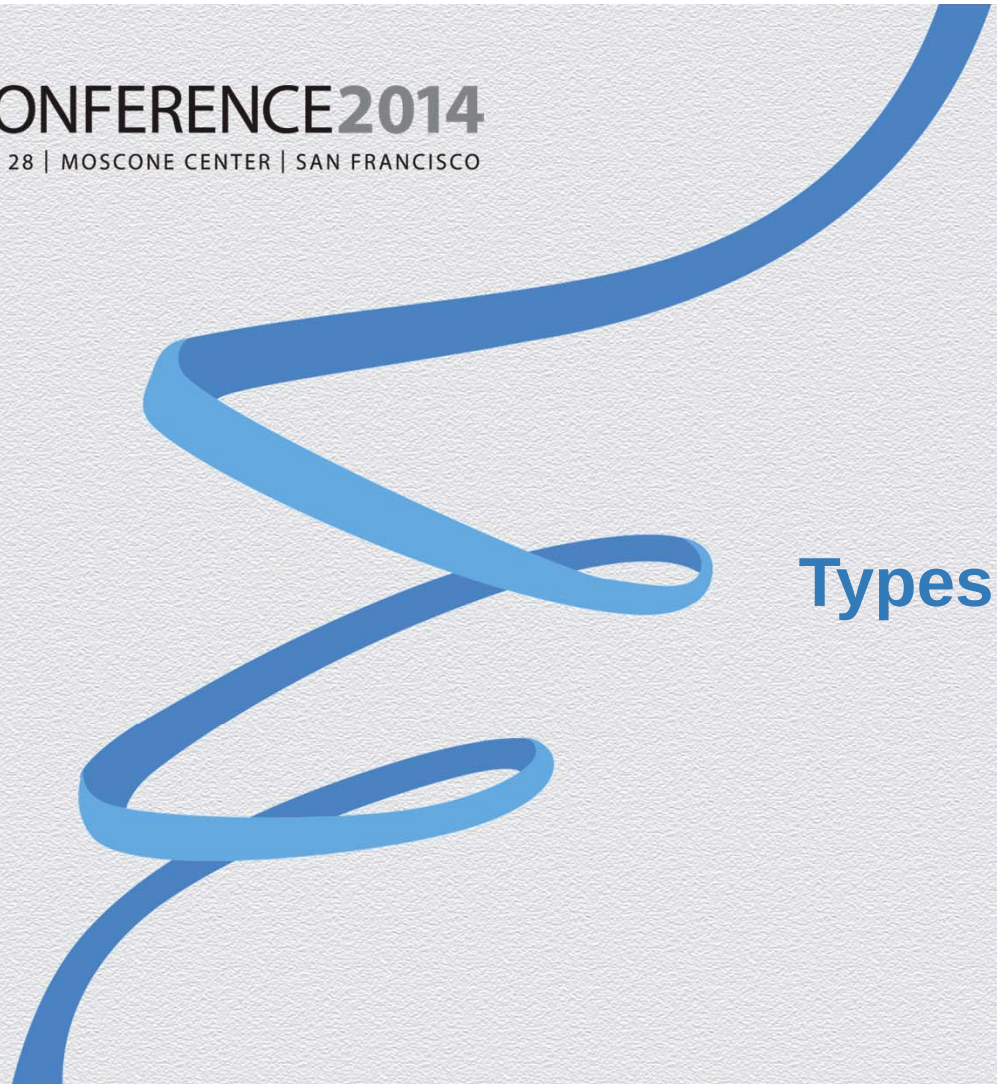
Virtual Private Networks



OpenDNS

VPN: Advantages/Disadvantages

- Advantages
  - Provide overall encryption
  - Allow you to remotely use protocols that are difficult to secure any other way
- Disadvantages
  - Involve dangerous network connections
  - Extend the network that you now have to protect



Types of Firewalls

Packet Filtering	Stateful Inspection	Application Proxy	Guard	Personal Firewall
Simplest	More complex	Even more complex	Most complex	Similar to packet filtering firewall
Sees only addresses and service protocol type	Can see either addresses or data	Sees full data portion of packet	Sees full text of communication	Can see full data portion of packet
Auditing difficult	Auditing possible	Can audit activity	Can audit activity	Can—and usually does—audit activity
Screens based on connection rules	Screens based on information across packets—in either header or data field	Screens based on behavior of proxies	Screens based on interpretation of message content	Typically, screens based on information in a single packet, using header or data
Complex addressing rules can make configuration tricky	Usually preconfigured to detect certain attack signatures	Simple proxies can substitute for complex addressing rules	Complex guard functionality can limit assurance	Usually starts in "deny all inbound" mode, to which user adds trusted addresses as they appear

So move on from Firewalls – what is NGFW?

- Non-disruptive in-line bump-in-the-wire configuration
- Standard first generation firewall capabilities
- Integrated signature-based IPS
- Application awareness\Ability to incorporate information from outside the firewall
- Upgrade paths to include future information feeds
- SSL Decryption

OpenDNS

Firewalls cannot....

- Protect your network against traffic that does not go through it
- Protect your company against completely new threats
- Protect your data if it cannot understand it
- Set itself up correctly
- Prevent revealing sensitive information through social engineering
- Protect against what has been authorized
- Secure against tunneling attempts

OpenDNS

Will the Firewall disappear with the perimeter?

- Is the Internet going to be the new corporate LAN?
- Where will the new “bump in the wire” be?
- Will the content & inspection approach still be relevant?

RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Firewalls & Perimeter Security

SESSION ID: SEM-M01

Dana Wolf

Sr. Director of Products, OpenDNS
@dayowolf

Security Basics

Sponsored by: CDNetworks

Start Time	Title	Presenter
8:30 AM	Introduction	Hugh Thompson
8:45 AM	Security Industry and Trends	Hugh Thompson
9:30 AM	Authentication Technologies	Michael Poitner
10:15 AM	Break	
10:30 AM	Governance, Risk and Compliance	Dennis Moreau
11:15 AM	Application Security	Jason Brvenik
12:00 PM	Lunch	
1:15 PM	Crypto 101/Encryption Basics, SSL & Certificates	Benjamin Jun
2:00 PM	Firewalls and Perimeter Protection	Dana Wolf
2:45 PM	Break	
3:00 PM	Viruses, Malware and Threats	Tas Giakouminakis
3:45 PM	Mobile and Network Security	Mike Janke

RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

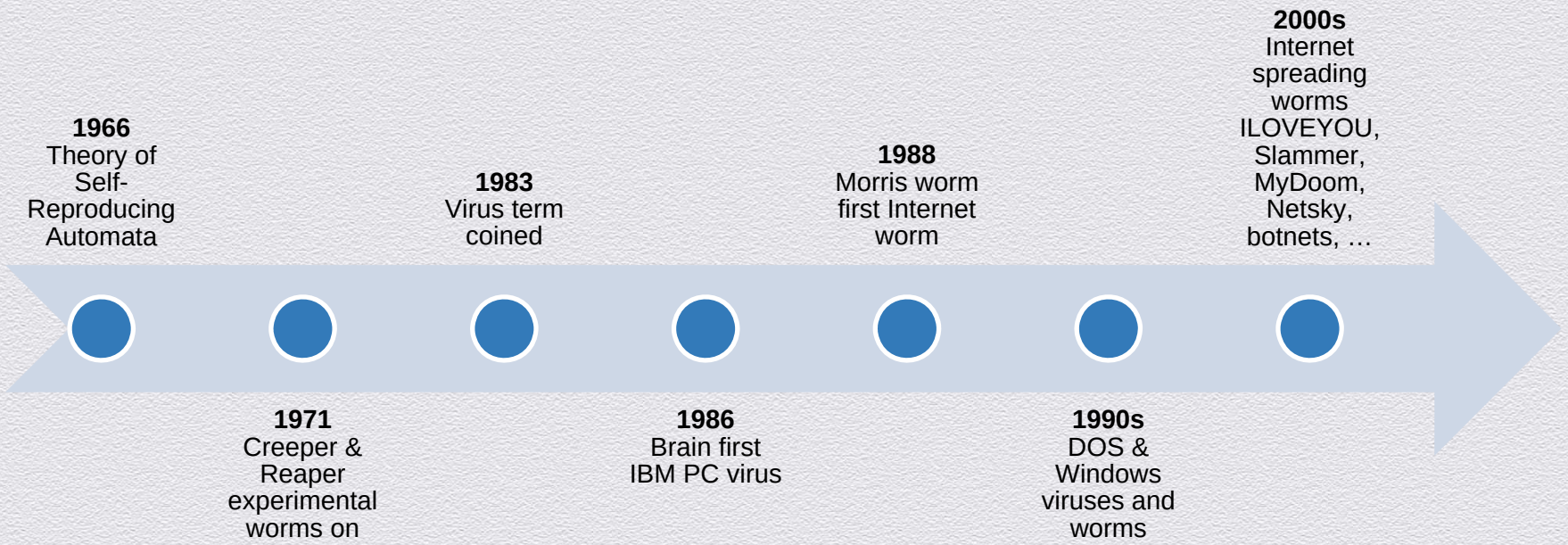
Security Basics Seminar
Viruses, Malware and Threats

SESSION ID: SEM-M01

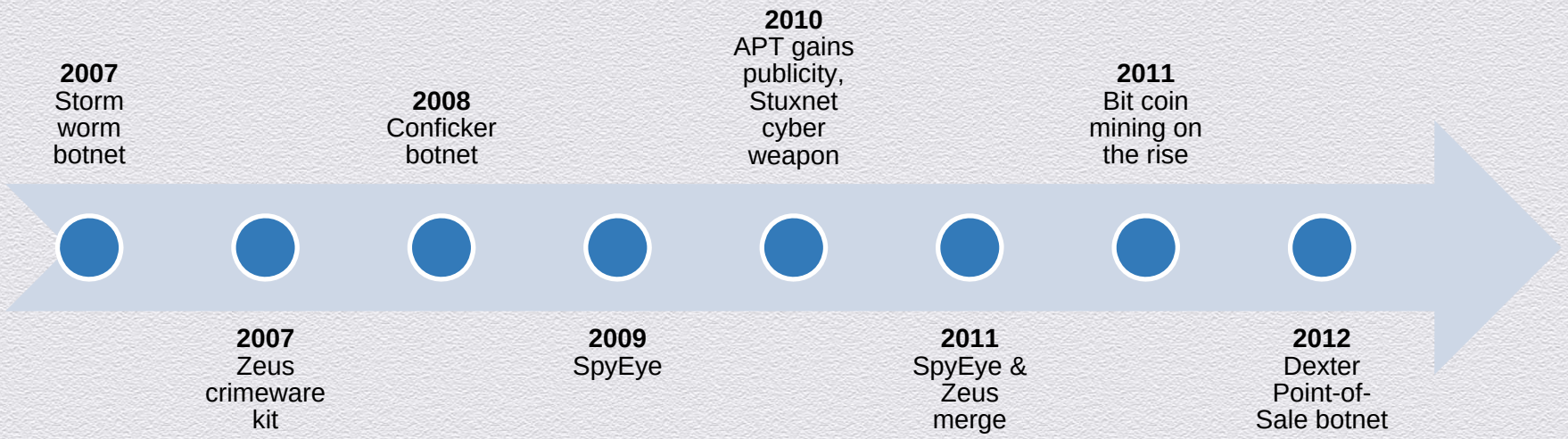
Tas Giakouminakis

Co-Founder & Chief Technology Officer
Rapid7

The Beginning

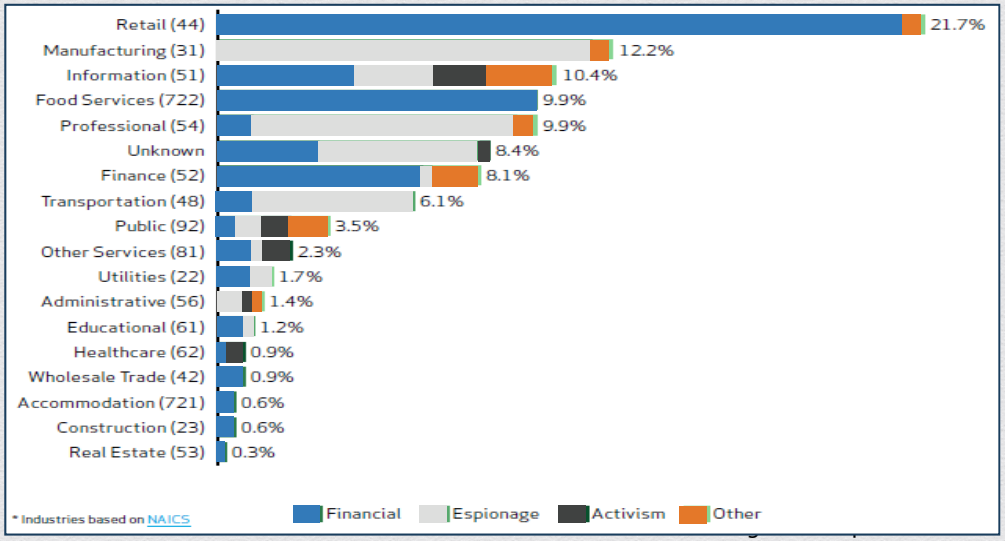


The Evolution



Threats, threats, everywhere

- Common threats impact everyone
  - Mass malware
  - “Unintentional” insiders
- Gain insight into industry specific threats
  - ISACs
  - UK CISP
  - Vendors



Verizon – 2013 Data Breach Investigations Report

RAPID7

#RSAC

RSACONFERENCE2014

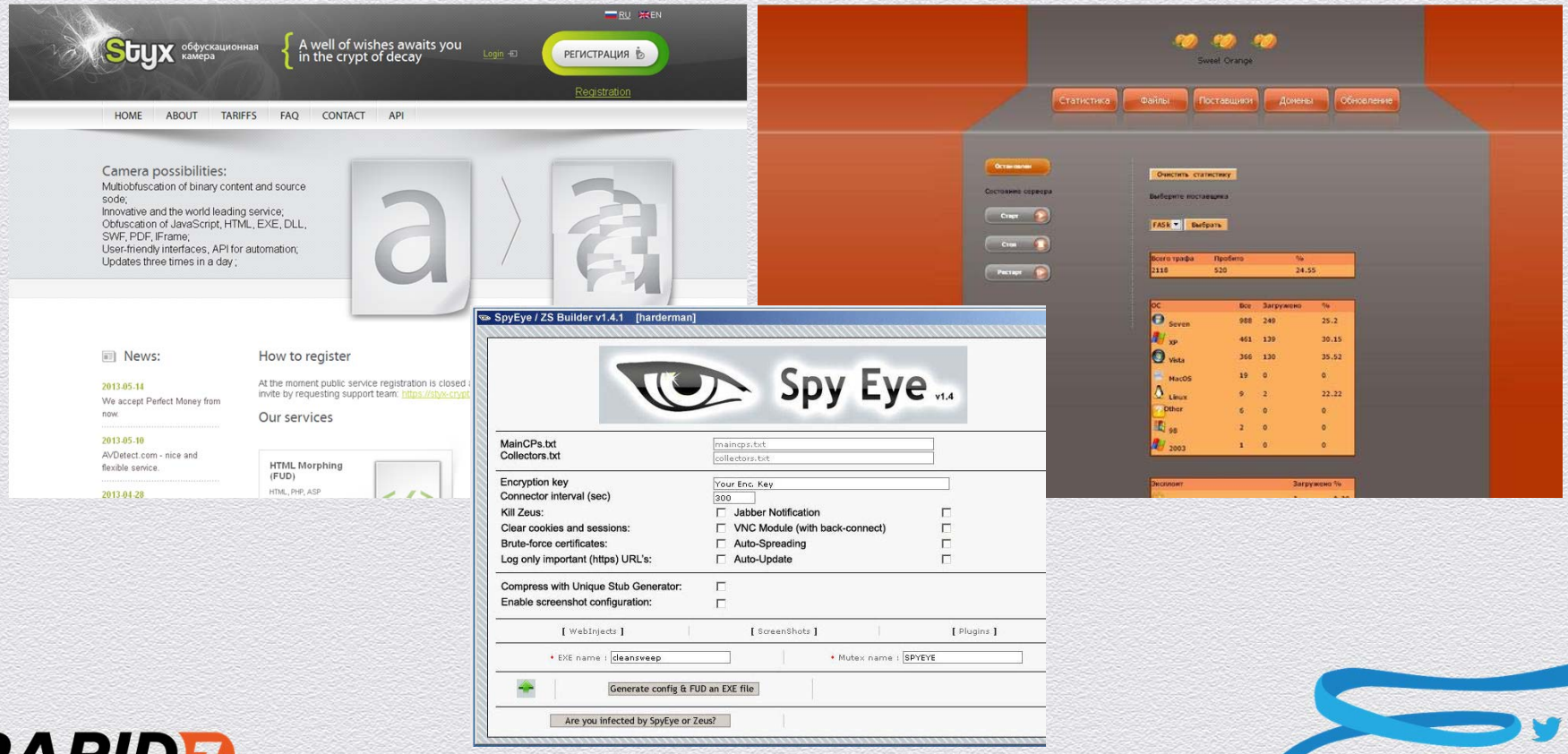
Know Your Enemy

- Hacktivists
- Cybercriminals
- State-Sponsored

Professions in Cyber Crime

- Intruders
- Malware Developers
- Exploit Kits Developers
- Bulletproof Hosting
- Money Laundering Providers
- Traffic Brokers
- …

Malware: There's an App For That



Goal: Making Money

Data/Service	Price Range
Credit Card # & CVV	$4-$8 (US) $7-$13 (UK/Australia/Canada) $15-$18 (EU/Asia)
Credit Card including track data	$12 (US) $19-$20 (UK/Australia/Canada) $28 (EU/Asia)
Fullz (identity and financial info)	$25 (US) $30-$40 (UK/Australia/Canada/EU/Asia)
Bank Account $70K-$150K	< $300
Infected Computers (1,000 – 15,000)	$20 - $250

Source: http://www.secureworks.com/resources/blog/the-underground-hacking-economy-is-alive-and-well/

It’s Not Just Endpoints

- Stuxnet made targeted SCADA/ICS attacks infamous
- Point-of-Sale malware on the rise
- ATM malware

Combating Today's Attacks

- Philosophy shifting from prevention to detection and containment
- Attackers increasingly rely on deception and the human element
- Intrusion Kill Chains – understand attackers methodology and apply corresponding defensive measures to increase cost/complexity to attacker

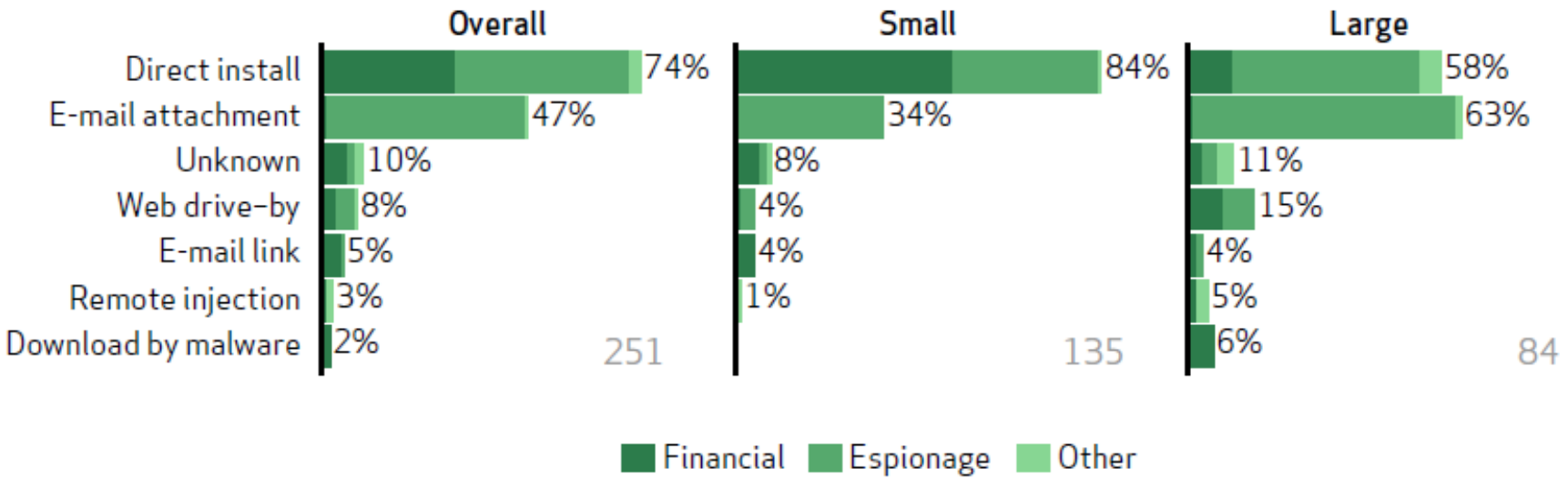
http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

The Intrusion Kill Chain

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command & Control (C2)
- Actions on Objectives

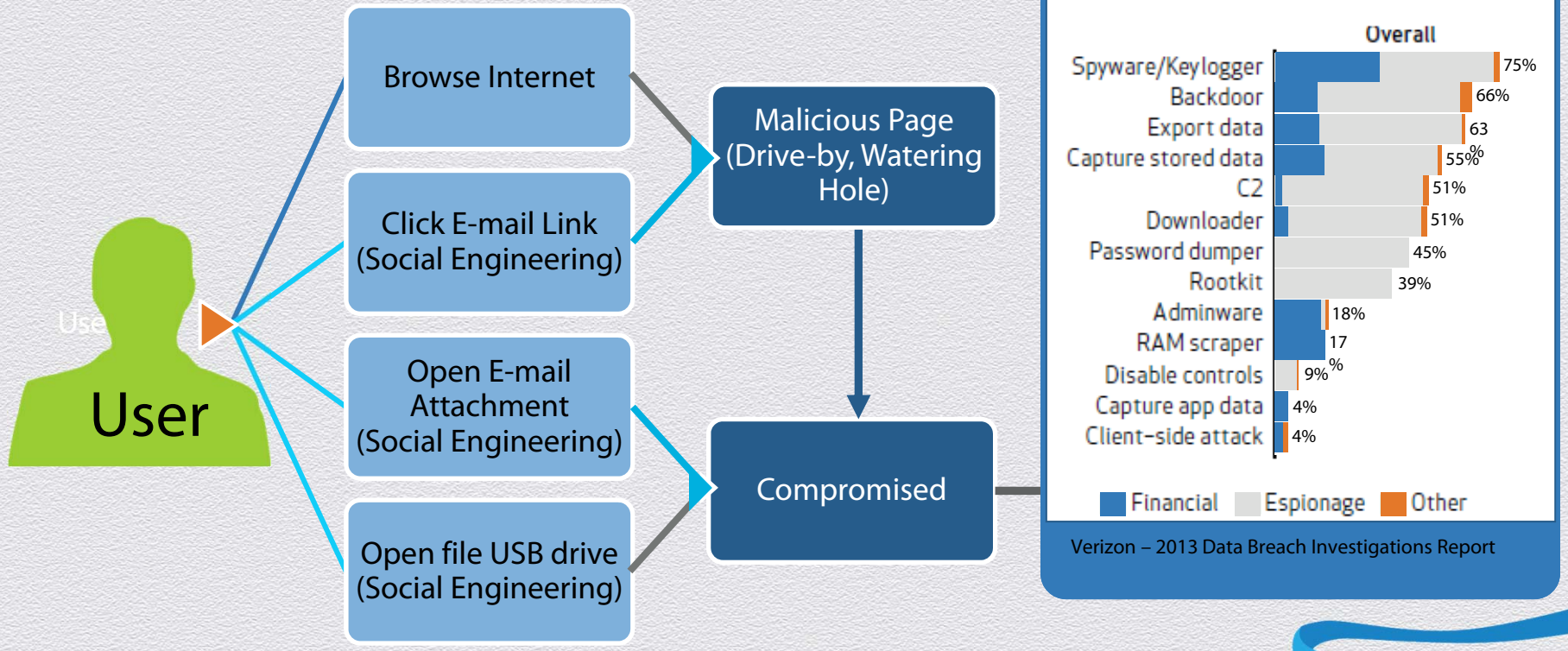
Malware Exposure

Figure 20: Vector for malware actions

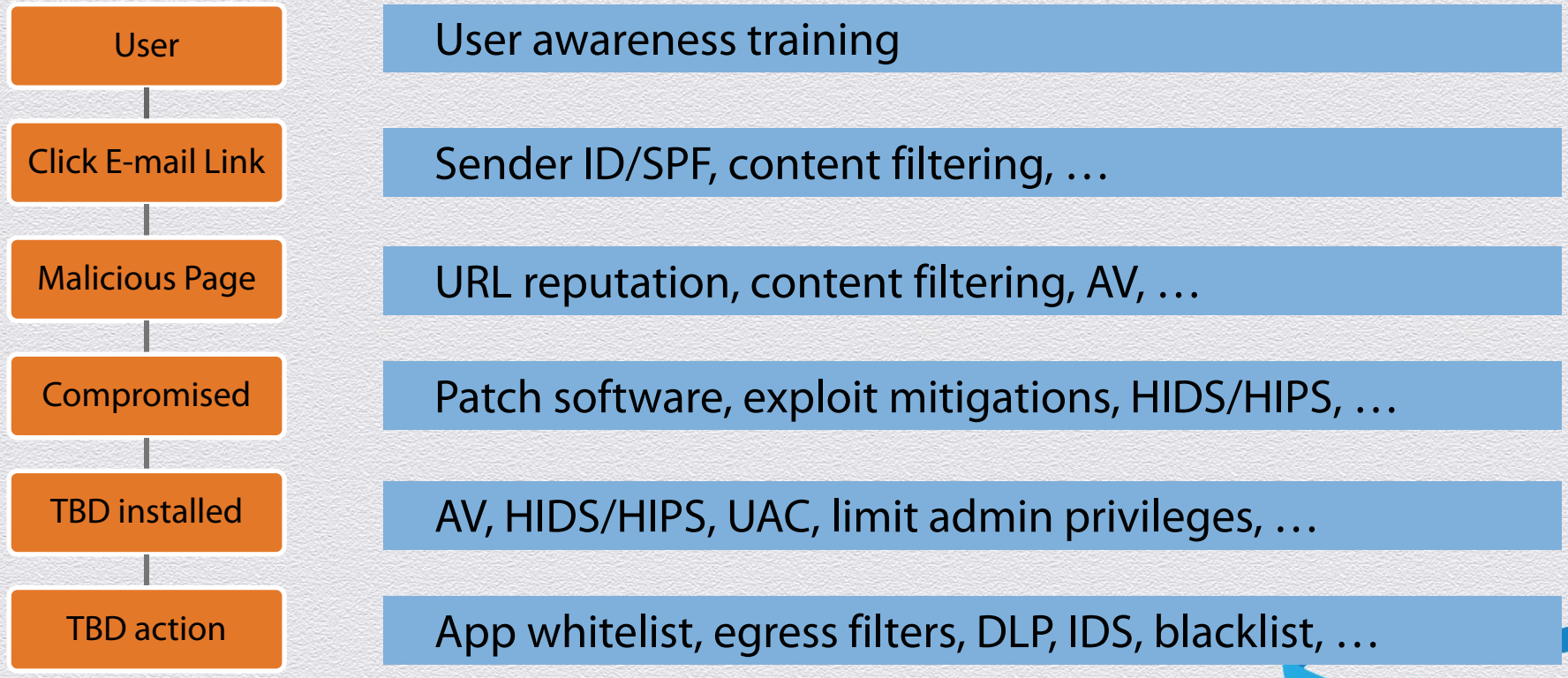


Verizon – 2013 Data Breach Investigations Report

User Targeted Attacks



Defending Against User Targeted Attacks



Additional Reading

Final Thoughts

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Thank You

Tas Giakouminakis

Rapid7

Co-founder & Chief Technology Officer

www.rapid7.com

tas@rapid7.com

Security Basics

Sponsored by: CDNetworks

Start Time	Title	Presenter
8:30 AM	Introduction	Hugh Thompson
8:45 AM	Security Industry and Trends	Hugh Thompson
9:30 AM	Authentication Technologies	Michael Poitner
10:15 AM	BREAK	
10:30 AM	Governance, Risk and Compliance	Dennis Moreau
11:15 AM	Application Security	Jason Brvenik
12:00 PM	LUNCH	
1:15 PM	Crypto 101/Encryption Basics, SSL & Certificates	Benjamin Jun
2:00 PM	Firewalls and Perimeter Protection	Dana Wolf
2:45 PM	Break	
3:00 PM	Viruses, Malware and Threats	Tas Giakouminakis
3:45 PM	Mobile and Network Security	Mike Janke

RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

MOBILE SECURITY

How did we get here? What is it? Where are we going?

SESSION ID: SEM-M01

Mike Janke
CEO & Co-Founder
Silent Circle

A Journey of Disruption

2014 is About the Past

IT Departments in 2007

- The iPhone just launched
- There were no app stores, no clouds (to speak of)
- 92% of all connected devices ran MSFT
- The new “Innovative” mobile devices
  - Blackberry rules the corporate world
  - Handspring, Nokia N, Danger Sidekick, Palm

IT Departments Were GODs

- Most company functions revolved around IT
  - From ERP systems, to email, to all communications
- CEO's and CFO's bowed down before them…
- Microsoft owned the world…Blackberry followed

The Winds of Change - Disruption

- Cloud Computing + Apps + Moore's Law pushing further
- Lightweight laptops, faster devices, Smarter Phones
- The "consumerization" of technology
- PC Hackers & Data Mining moved to Mobile – fertile hunting grounds

You Became The Customer

- The end customer became YOU, not IT
- C-Suite Executives brought more efficient devices to work
- BYOD begins to happen
- iPhone 3GS (2009)
- iPad (2010) with Microsoft ActiveSync

Users Begin Dictating Products to the Enterprise

- Politicians, CEO's, Sales Executives, "Cool" is also efficient
- Executives bring iPads, Androids, iPhones, slim laptops to work
- "I don't care –find a way to make it work", IT is told
- Hundreds of Apps –more efficient + cheaper than existing infrastructure in enterprises
- Efficiency soars, IT goes from buying equipment to integrating

What is Mobile Security?

Uhmmm...

It’s being free from someone stealing your stuff

It’s Safety

It’s Control

What is Mobile Security?

- Ultimately: Mobile Security is about CONTROL for Enterprise
  - AND about securing “your stuff” as a consumer
- The FRICTION POINT happens when CONTROL hits “Your Stuff”..

The Security Reality?

LET ME BE PERFECTLY CLEAR…

- There is no Bloke that can't be Beaten…
- No horse that can't be rode…

And NO PHONE THAT IS 100% SECURE….

So What Does Security Feel Like?

CONSUMER:

- Keep criminals out of my device. Its my money/data –not theirs…
- Let me decide who gets my data and when –including the Government

ENTERPRISE:

- Keep criminals, competitors & hackers out of “OUR” devices
- Give us control so we know what is going on…and IT stays employed
- We don’t want to end up in the “headlines on CNN”

Confusion & Fragmentation

CONSUMER:

- Who has my data? Everyone!!! How come I didnt know?
- I want the magic of technology and I don't want to think of security

ENTERPRISE:

- MDM? MAM? Zero Days, Malware, 52 vendors, 27 solutions, BYOD?
- I need to control ALL devices, but I can't –always playing "catch-up".

Who Dictates the Future of Mobile?

FOLLOW THE MONEY….

- The Customer changed
- It used to be IT Departments
- Now it's the end consumer…BYOD

Products *flow* from the user…
To the Enterprise

Mobile Devices are *at least* as secure as the desktop and laptops they augment

- Code signing + Sandboxing + better integrated security hardware
- IOS's mini HSM
- ARM Trustzone
- Apps are safer than websites…less cross-site contamination

They Have Much Less…

- Data archives with decades of data
- Files more focused to on-going tasks
- Email is a subset of messages

Better Remediation

- Device Encryption (on by default with IOS)
- Remote wipe – Baseband makes this easier

Why is it so hard to solve these problems?

- Phone, Chip and Hardware companies go for $$$, not security
- Governments go for surveillance and regulations
- Consumers go for convenience

SILENT CIRCLE

Where is The Next Disruption?

Mobile Device Monopolies are about to hit a wall (Apple, Samsung)

- Smartphone saturation is coming….HTC/LG/BB/Nokia all losing $$
- Smaller innovative specialty & niche makers are servicing areas the giants cannot…Security/Style/Customization (Xiaomi and others)

Consolidation of Mobile Security Services

- One-stop shops coming (MDM, Secure Comms, Hardware, Cloud)
- Too much funding for too many solutions…too much security “noise”

ACTIONABLE ADVICE

Products flow from the user up to the enterprise – not vice versa

- Device makers know who the customer is… security is not a priority
- Control products are starting to flow to the platform

Security depends upon what “you” want…. control or safety

- We are in the midst of a revolution… users want more “privacy control”
- Consolidation of products/services and security disruption is just NOW beginning.
- Don’t try to solve everything – start with basics – change is too quick